

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: Chan-Wah NG, et al.
Application No.: New PCT National Stage Application
Filed: April 14, 2005
For: ROAMING CONNECTION METHOD AND APPARATUS IN
GLOBAL NETWORK

CLAIM FOR PRIORITY

Assistant Commissioner of Patents
Washington, D.C. 20231

Dear Sir:

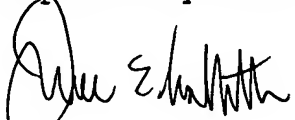
The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. No. 2002-303879, filed October 18, 2002.

The International Bureau received the priority document within the time limit, as evidenced by the attached copy of the PCT/IB/304.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,


James E. Ledbetter
Registration No. 28,732

Date: April 14, 2005

JEL/spp

Attorney Docket No. L9289.05123
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L STREET, NW, Suite 850
P.O. Box 34387
WASHINGTON, DC 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

日 本 国 特 許 庁
JAPAN PATENT OFFICE

10.11.03

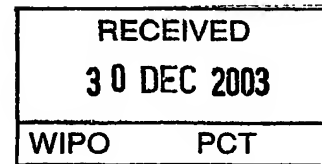
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 8 日
Date of Application:

出 願 番 号 特 願 2 0 0 2 - 3 0 3 8 7 9
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 0 3 - 8 7 9]

出 願 人 松下電器産業株式会社
Applicant(s):

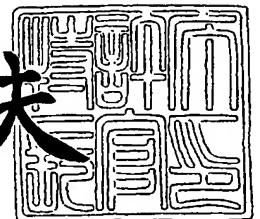


**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2 0 0 3 年 1 2 月 1 1 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 2900645251
【特記事項】 特許法第36条の2第1項の規定による特許出願
【あて先】 特許庁長官殿
【国際特許分類】 G06F 13/00

H04L 12/46

H04L 12/28

H04L 12/66

【発明者】

【住所又は居所】 シンガポール 534415 シンガポール、タイ・セン・アベニュー、ブロック 1022、04-3530 番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】 チャン ワー・ン

【発明者】

【住所又は居所】 シンガポール 534415 シンガポール、タイ・セン・アベニュー、ブロック 1022、04-3530 番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】 ペク ユー・タン

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100093067

【弁理士】

【氏名又は名称】 二瓶 正敬

【手数料の表示】

【予納台帳番号】 039103

【納付金額】 35,000円

【提出物件の目録】

【物件名】 外国語明細書 1

【物件名】 外国語図面 1

【物件名】 外国語要約書 1

【包括委任状番号】 0003222

【プルーフの要否】 要

【書類名】 外国語明細書

1 Title of the Invention

Method and Apparatus of provisioning global connectivity to roaming networks

2 Claims

1. A method of provisioning global connectivity to roaming networks, used in an internetworking of packet-switched data communications networks, wherein network elements in the communications networks are uniquely addressed by a primary global address such that the network element can be reached even when it is roaming anywhere in the communication networks, whereas the network elements that are roaming within the communications networks can be additionally assigned with a temporary global address for a duration of which the roaming network element is attached to a single access router, through which the roaming network element gains access to a global data communications network, comprising the step of sending a Binding Updates message from the roaming network element to a singular or plural other network elements, wherein the Binding Update message contains the primary global address and the temporary global address of the sending roaming network element, for which the objective is to allow the receiving network elements relate the specified temporary global address to the specified primary global address, and further contains the primary global address of the access router to which the roaming network element is currently attached.

2 The method of provisioning global connectivity to roaming networks according to claim 1, wherein the network element in the internetworking of packet-switched data communications networks attaches a data format

onto the Binding Update message in order to insert the primary global address of the access router to which the roaming network element is attached in the Binding Update message, the data format comprising:

- i. a type field to identify the data format as containing the primary global address of the access router to which the sender is attached;
- ii. a length field to specify a length of the data format; and
- iii. an access-router-address field to contain the primary global address of the access router to which the sender is attached.

3 The method of provisioning global connectivity to roaming networks according to claim 1, wherein the access router in the internetworking of packet-switched data communications networks attaches a data format on to advertisement messages sent to advertise its service as the access router in order to insert its primary global address in the advertisement messages, the data format comprising:

- i. a type field to identify the data format as containing the primary global address of the sender;
- ii. a length field to specify a length of the data format; and
- iii. an access-router-address field to contain the primary global address of the sender.

4 A method of provisioning global connectivity to roaming networks, used between a plurality of the network elements in the internetworking of packet-switched data communications networks, wherein one of the network elements is roaming in the internetworking of packet-switched data communications networks, comprising the steps of:

- i. sending a Binding Update message from the roaming network element to another network element, wherein the Binding Update message contains a pre-determined primary global address and a temporary global address

additionally assigned of the sending roaming network element, for which the objective is to allow the receiving network element relates the specified temporary global address to the specified primary global address, and further contains the primary global address of an access router to which the roaming network element is currently attached, and;

ii. replying from the recipient of the Binding Update message to the roaming network element with a Binding Acknowledgement message, wherein the Binding Update message contains information on whether the Binding Update message is accepted or rejected, and further contains an indication the presence of which serves to inform the recipient of the Binding Acknowledgement message that the sender of the Binding Acknowledgement message can understand and can take appropriate action on the inclusion of the primary global address of the access router in the Binding Update message.

5 The method of provisioning global connectivity to roaming networks according to claim 1, wherein a network entity can record the Binding Update message in Binding Entries when the network entity received the Binding Update message, the Binding Entries consisting of the following fields:

- i. Home-Address field, which contains the primary global address of the roaming network element;
- ii. Care-Of-Address field, which contains the temporary global address of the roaming network element; and
- iii. Access-Router-Address field, which contains the primary global address of the access router to which the roaming network element is attached.

6 A method of provisioning global connectivity to roaming networks ac

according to claim 5, which the network entity performs to update the Binding Entries when the network entity received the Binding Update message, comprising the steps of:

i. checking if the Binding Entries contains an entry with the Home-Address field equal to the primary global address specified in the received Binding Update message, and creating a new entry if one is not found ;

ii. deleting the entry in the Binding Entries which has the Home-Address field equal to the primary global address specified in the received Binding Update message if it does not contain any information on the temporary global address of the sender of the Binding Update message;

iii. deleting the entry in the Binding Entries which has the Home-Address field equal to the primary global address specified in the received Binding Update message if the information on the temporary global address contained in the Binding Update message equal to the Home-Address field in the entry;

iv. setting the Care-of-Address field of the entry to the temporary global address specified in the received Binding Update message, if there is the temporary global address contained in the received Binding Update message and its value is not the same as the Home-Address field in the entry;

v. setting the Access-Router-Address field of the entry to the primary global address of the access router specified in the Binding Update message if there is one; and

vi. setting the Access-Router-Address field of the entry to be invalid if the received Binding Update message does not contain any information on the primary global address of the access router.

7 The method of provisioning global connectivity to roaming networks

according to claim 5, which the network element performs to construct a routing header attached to a data packet, wherein the routing header is used to instruct the network element addressed by the destination address specified in the packet to forward the packet to another destination, comprising the steps of:

- i. initialising a last-in-first-out data structure to be empty and a temporary variable to store the primary global address of a final destination of the packet;
- ii. finding an entry in the Binding Entries wherein the Home-Address field of the entry contains the same address stored in the aforementioned temporary variable;
- iii. storing the value in the temporary variable to the top of the last-in-first-out data structure if the value equals to the primary global address of the final destination of the packet in case that the entry in the Binding Entries is found;
- iv. storing the value contained in the Care-of-Address field of the entry in the temporary variable in case that the entry in the Binding Entries is found;
- v. storing the value in the temporary variable to the top of the last-in-first-out data structure and then storing the value in the Access-Router-Address field of the entry to the temporary variable in case that the entry in the Binding Entries is found,
- vi. repeating the steps (ii), (iii), (iv) and (v) if the Access-Router-Address field of the entry is valid;
- vii. repeatedly removing the top value in the last-in-first-out data structure and appending the removed value to the routing header attached to the data packet until the last-in-first-out data structure is empty in case that the entry in the Binding Entries is found or the Access-Router-Address field of the found entry is not valid; and

viii. setting the destination address of the data packet to the value stored in the temporary variable.

8 The method of provisioning global connectivity to roaming networks according to claim 1, further comprising the step of inserting a unique signal on a data packet to request the access router to which the network element is attached, to forward the data packet sent by the network element directly to the destination specified in the data packet.

9 The method of provisioning global connectivity to roaming networks according to claim 1, further comprising the step of invalidating the unique signal defined in claim 8 on a data packet to prevent subsequent intermediate routers to forward the data packet directly to the destination specified in the data packet.

10 The method of provisioning global connectivity to roaming networks according to claim 8, which an intermediate network element in the internetworking of packet-switched data communications networks performs to process a data packet received from its ingress interface, wherein the intermediate network element serves as a router bridging a singular or plural local data communication networks in its ingress interface to the internetworking of packet-switched data communications networks in its egress interface, comprising the steps of:

i. forwarding the received packet if the intermediate network element is not roaming in the internetworking of packet-switched data communications networks;

ii. encapsulating the received packet in another newly created packet to be sent to a specific network element in the internetworking of packet-switched data communications networks, where the specific network

element will extract the original data packet from the newly created packet and forward it to the destination, if the received packet does not contain any unique signal or if the unique signal is invalidated, in case that the intermediate network element is roaming in the internetworking of packet-switched data communications networks and assigned the temporary global address;

iii. encapsulating the received packet in another newly created packet to be send to the specific network element in the internetworking of packet-switched data communications networks, where the specific network element will extract the original data packet from the newly created packet and forward it to the destination, if a source address specified on the received packet is not a valid address in the local network of the ingress interface of the intermediate network element, in case that the intermediate network element is roaming in the internetworking of packet-switched data communications networks and assigned the temporary global address;

iv. encapsulating the received packet in another newly created packet to be send to the specific network element in the internetworking of packet-switched data communications networks, where the specific network element will extract the original data packet from the newly created packet and forward it to the destination, if the destination address specified on the received packet has not been sent any Binding Update message by the intermediate network element, wherein the Binding Update message contains the primary global address and the current temporary global address of the intermediate network element in case that the intermediate network element is roaming in the internetworking of packet-switched data communications networks and assigned the temporary global address,; and

v. changing the source address of the received packet to the tempor

ary global address of the intermediate network element and then forwarding the received packet to the specified destination, if the received packet contains the unique signal, and if the source address specified on the received packet is a valid address in the local network of the ingress interface of the intermediate network element, and if the destination address specified on the received packet has previously been sent the Binding Update message by the intermediate network element, wherein the Binding Update message contains the primary global address and the current temporary global address of the intermediate network element in case that the intermediate network element is roaming in the internetworking of packet-switched data communications networks and assigned the temporary global address.

11 The method of provisioning global connectivity to roaming networks according to claim 5, which the network element in the internetworking of packet-switched data communications networks performs to verify if a source address specified in a received data packet addressed to the network element is legitimate, wherein the received data packet contains information on the primary global address of the access router, to which the originator of the received packet is attached, that is different from the source address specified in the received data packet, comprising the steps of:

- i. initialising a temporary variable to store the primary global address contained in the received data packet;
- ii. declaring the source address to be legitimate, if the value stored in the temporary variable equals to the source address specified in the data packet;
- iii. searching for an entry in the Binding Entries with the value in the Home-Address field equal to the value stored in the temporary vari

able in case that the value stored in the temporary variable does not equal to the source address specified in the data packet;

iv. declaring the source address to be illegitimate if an entry in the Binding Entries with the value in the Home-Address field equal to the value stored in the temporary variable cannot be found in case that the value stored in the temporary variable does not equal to the source address specified in the data packet,;

v. declaring the source address to be legitimate if the Care-of-Address field of an entry in the Binding Entries contains a value equal to the source address specified in the data packet in case that an entry in the Binding Entries is found;

vi. declaring the source address to be illegitimate if the Access-Router-Address field of the entry is invalid in case that an entry in the Binding Entries is found and the Care-of-Address field of the entry contains a value not equal to the source address specified in the data packet;

vii. storing the contents in the Access-Router-Address field of the entry in the temporary variable in case that an entry in the Binding Entries is found and the Care-of-Address field of the entry contains a value not equal to the source address specified in the data packet; and

viii repeating the steps (iii), (iv), (v), (vi), and (vii) if the Access-Router-Address field of the entry is valid.

12 The method of provisioning global connectivity to roaming networks according to claim 1, to send a data packet containing a routing header, wherein the method is used after a successful reception of the Binding Update message containing the primary global address of the access router to which the sender of the Binding Update message is attached, comprising the steps of:

- i. setting the source address of the data packet to be the primary global address of the access router; and
- ii. setting the routing header to contain only the temporary global address and primary global address of the sender of the Binding Update message.

13 The method of provisioning global connectivity to roaming networks according to claim 1, to send a data packet containing a routing header, wherein the method is used after a successful reception of the Binding Update message containing the primary global address of the access router to which the sender of the Binding Update message is attached, comprising the steps of:

- i. setting the source address of the data packet to be the primary global address of the access router; and
- ii. setting the routing header to contain the temporary global address of the sender of the Binding Update message as a first entry.

14 The method of provisioning global connectivity to roaming networks according to claim 1, to send a data packet containing a routing header, wherein the method is used after a successful reception of a first Binding Update message which is sent by the network element, the first Binding Update message containing the primary global address of the access router to which the sender of the Binding Update message is attached, and after a successful reception of a second Binding Update message which is sent by the access router, the second Binding Update message containing the temporary global address of the access router, comprising the steps of:

- i. setting the source address of the data packet to be the temporary global address of the access router; and

ii. setting the routing header to contain the temporary global address and primary global address of the sender of the first Binding Update message.

15 The method of provisioning global connectivity to roaming networks according to claim 1, to send a data packet containing a routing header, wherein the method is used after a successful reception of a first Binding Update message which is sent by the network element, the first Binding Update message containing the primary global address of the access router to which the sender of the Binding Update message is attached, and after a successful reception of a second Binding Update message which is sent by the access router, the second Binding Update message containing the temporary global address of the access router, comprising the steps of:

i. setting the source address of the data packet to be the temporary global address of the access router; and

ii. setting the routing header to contain the temporary global address of the sender of the first Binding Update message as a first entry.

16 The method of provisioning global connectivity to roaming networks according to claim 1, to send a data packet containing a routing header, wherein the method is used after a successful reception of a first Binding Update message which is sent by the network element, the first Binding Update message containing the primary global address of the access router to which the sender of the Binding Update message is attached, and after a successful reception of a second Binding Update message which is sent by the access router, the second separate Binding Update message containing the temporary global address of the access router, comprising the step of setting the routing header to contain the temporary global

address of the sender of the first Binding Update message and the temporary global address of the access router, wherein the temporary address of the access router appears immediately before the temporary global address of the sender of the first Binding Update message in the routing header.

17 The method of provisioning global connectivity to roaming networks according to claim 8, wherein the network element is roaming in the internetworking of communications network and is serving as a router bridging a singular or plural local data communication networks in its ingress interface to the internetworking of packet-switched data communications networks in its egress interface, after receiving a data packet from its ingress interface, wherein the data packet contains the unique signal, comprising the steps of:

- i. changing a source address of the data packet to its temporary global address; and
- ii. forwarding the data packet to its egress interface.

18 An apparatus used by a network element in the internetworking of packet-switched data communications networks defined in claim 1, comprising means for executing the followings:

- i. the method of utilizing the Binding Entries as defined in claim 5;
- ii. the method of updating the Binding Entries as defined in claim 6;
- iii. the method of inserting an indication in a Binding Acknowledgement message, wherein the presence of such an indication serves to inform the recipient of the Binding Acknowledgement message that the sender can understand and can take appropriate action on the inclusion of the pr

primary global address of the access router in the Binding Update message, as defined in claim 4;

iv. the method of checking the source address of a data packet as defined in claim 8; and

v. the method of constructing a routing header, as defined in any one of claims 7, 13, 14, 15, and 16.

19 An apparatus used by a network element in the internetworking of packet-switched data communications networks defined in claim 1, wherein the network element is roaming in the internetworking of communications network, comprising means for executing the followings:

i. the method of utilizing the Binding Entries as defined in claim 5;

ii. the method of updating the Binding Entries as defined in claim 6;

iii. the method of inserting an indication in a Binding Acknowledgement message, wherein the presence of such an indication serves to inform the recipient of the Binding Acknowledgement message that the sender can understand and can take appropriate action on the inclusion of the primary global address of the access router in the Binding Update message, as defined in claim 4;

iv. the method of checking the source address of a data packet as defined in claim 11;

v. the method of constructing a routing header, as defined in claim 7;

vi. the method of inserting a signal on a data packet to request the access router to which the network element is attached, to directly forward the data packet directly to the destination specified in the data packet, as defined in claim 8; and

vii. the method of inserting the primary global address of the access router to which the network element is attached in the Binding Update message, as defined in claims 1 and 2.

20 An apparatus used by a network element in the internetworking of packet-switched data communications networks defined in claim 1, wherein the network element is roaming in the internetworking of communications network and is serving as a router bridging a singular or plural local data communication networks in its ingress interface to the internetworking of packet-switched data communications networks in its egress interface, comprising means for executing the followings:

i. the method of attaching information of the primary global address of the network element in advertisement messages as defined in claim 3 ;

ii. the method of utilizing the Binding Entries as defined in claim 5;

iii. the method of updating the Binding Entries as defined in claim 6;

iv. the method of inserting an indication in a Binding Acknowledgement message, wherein the presence of such an indication serves to inform the recipient of the Binding Acknowledgement message that the sender can understand and can take appropriate action on the inclusion of the primary global address of the access router in the Binding Update message, as defined in claim 4;

v. the method of checking the source address of a data packet as defined in claim 11;

vi. the method of constructing a routing header, as defined in claim 7;

vii. the method of inserting a signal on a data packet to request t

he access router to which the network element is attached, to directly forward the data packet directly to the destination specified in the data packet, as defined in claim 8;

viii. the method of inserting the primary global address of the access router to which the network element is attached in a Binding Update message, as defined in claims 1 and 2; and

ix. the method of processing data packet arriving from the ingress interface of the network element to be forwarded to the egress interface of the network element, as defined in claims 10 and 17.

3 Detailed Description of Invention

Industrial Field of Utilisation

The invention relates to the delivering of packets in the internetworking of packet-switched data communications networks. In particular, the disclosed invention addressed problems in the provisioning of connectivity to a network of nodes that is constantly changing its point of attachment to the global data communications network. This invention can be viewed as an enhancement to existing solutions for provisioning global connectivity to roaming hosts.

Background and Prior Art

Disclosure of Information on prior art documents

[Non-patent document 1] Soliman, H., and Pettersson, M., "Mobile Networks (MONET) Problem Statement and Scope", Internet Draft: draft-soliman-monet-statement-00.txt, Feb 2002, Work In Progress.

[Non-patent document 2] Ernst, T., and Lach, H., "Network Mobility Support Requirements", Internet Draft: draft-ernst-monet-requirements-00.txt, Feb 2002, Work In Progress.

[Non-patent document 3] Lach, H. et. al., "Mobile Networks Scenarios

, Scope and Requirements", Internet Draft: draft-lach-monet-requirements-00.txt, Feb 2002, Work In Progress.

[Non-patent document 4] Kniventon, T. J., and Yegin, A. E., "Problem Scope and Requirements for Mobile Networks Working Group", Internet Draft: draft-kniventon-monet-requiremetns-00.txt, Feb 2002, Work In Progress.

[Non-patent document 5] Perkins, C. E. et. al., "IP Mobility Support", IETF RCF 2002, Oct 1996.

[Non-patent document 6] DARPA, "Internet Protocol", IETF RFC 791, Sep 1981.

[Non-patent document 7] Johnson, D. B., Perkins, C. E., and Arkko, J., "Mobility Support in IPv6", Internet Draft: draft-ietf-mobileip-ipv6-18.txt, Work In Progress, June 2002.

[Non-patent document 8] Deering, S., and Hinden, R., "Internet Protocol Version 6 (IPv6) Specification", IETF RFC 2460, Dec 1998.

[Non-patent document 9] Simpson, W., "IP in IP Tunneling", IETF RFC 1853, Oct 1995.

[Non-patent document 10] Conta, A., and Deering, S., "Generic Packet Tunneling in IPv6", IETF RFC 2473, Dec 1998.

[Non-patent document 11] Kniveton, T., "Mobile Router Support with Mobile IP", Internet Draft: draft-kniveton-mobrtr-01.txt, Work In Progress, Mar 2002.

[Non-patent document 12] Thubert, P., and Molteni, M., "IPv6 Reverse Routing Header and Its Application to Mobile Networks", Internet Draft: draft-thubert-nemo-reverse-routing header-00.txt, Work In Progress, Jun 2002.

[Non-patent document 13] Ernst, T., Castelluccia, C., Bellier, L., Lach, H., and Olivereau, A., "Mobile Networks Support in Mobile IPv6 (Prefix Scope Binding Updates)", Internet Draft: draft-ernst-mobileip-v6-ne

work-03.txt, Mar 2002.

[Non-patent document 14] Narten, T., Nordmark, E., and Simpson, W., "Neighbour Discovery for IPv6", IETF RFC 2461, Dec 1998.

The Internet today has evolved to a stage where numerous peripheral data communications networks are deployed around a system of fixed network nodes. These peripheral networks are suitably known as edge networks; whereas the system of fixed network nodes surrounded by the edge networks are known as the core. With the emergence and proliferation of wireless technology, more and more of these edge networks are employing wireless solution, thus forming a special edge network called mobile networks, or network in motion [Non-patent document 1,2,3,4].

In essence, a mobile network is a network of nodes where the entire network changes its point of attachment to the Internet. This usually entails a mobile router (which bridge the mobile network to the Internet) in the mobile network that changes its point of attachment to the Internet between different access routers (which may, in fact, be mobile themselves). Examples of mobile networks include networks attached to people (known as Personal Area Network, or PAN) and networks of sensors deployed in vehicles such as cars, trains, ships or aircrafts. For mass transport systems such as airplanes, trains, or buses, the operators may provide passengers with permanent on-board Internet access allowing them to use their laptops, Personal Digital Assistants (PDA), or mobile phones to connect to remote hosts. Individual nodes in such a mobile network are usually connected to a central device (i.e. the mobile router), and do not change their attachment when the network is in motion. Instead, it is the mobile router that changes its point of attachment as the network moves in entirety.

This invention describes a proposed solution for the problem of network in motion. In essence, the problem of network in motion is to provide

continuous Internet connectivity to nodes in a network that moves as a whole. Nodes within the network that moves may not be aware of the network changing its point of attachment to the Internet. This differs from the traditional problem of mobility support as addressed by Mobile IPv4 [Non-patent document 5] in Internet Protocol version 4 (IPv4) [Non-patent document 6] and Mobile IPv6 [Non-patent document 7] in Internet Protocol version 6 (IPv6) [Non-patent document 8]. In [Non-patent document 5, 7], the main objective is to provide mobility support to individual hosts rather than an entire network.

In Mobile IP, each mobile node has a permanent home domain. When the mobile node is attached to its home network, it is assigned a permanent global address known as a home-address. When the mobile node is away, i.e. attached to some other foreign networks, it is usually assigned a temporary global address known as a care-of-address. The idea of mobility support is such that the mobile node can be reached at the home-address even when it is attached to other foreign networks. This is done in [Non-patent document 5, 7] with an introduction of an entity at the home network known as a home agent. Mobile nodes register their care-of-addresses with the home agents using messages known as Binding Updates. The home agent is responsible to intercept messages that are addressed to the mobile node's home-address, and forward the packet to the mobile node's care-of-address using IP-in-IP Tunnelling [Non-patent document 9, 10]. IP-in-IP tunnelling involves encapsulating an original IP packet in another IP packet. The original packet is sometimes referred to as the inner packet, and the new packet that encapsulates the inner packet is referred to as the outer packet.

Extending the concept of mobility support for individual hosts to mobility support for a network of nodes, the objective of a network in motion solution is to provide a mechanism where nodes in a mobile network can

be reached by their permanent addresses, no matter where on the Internet the mobile network is attached to. There exist a few prior attempts to solve the network in motion problem, all of them are based on Mobile IP [Non-patent document 5,7].

One proposed solution for network in motion is the Mobile Router Support [Non-patent document 11]. Here the mobile router controlling a mobile network performs routing of packets to and from the mobile network using some routing protocols when it is in its home domain. When the mobile router and its mobile network move to a foreign domain, the mobile router registers its care-of-address with its home agent. An IP-in-IP tunnel is then set up between the mobile router and the home agent. The routing protocol used when the mobile router is at its home domain is again performed over the IP-in-IP tunnel. This means that every packet going to the mobile network will be intercepted by the home agent and forwarded to the mobile router through the IP-in-IP tunnel. The mobile router then forwards the packet to a host in its mobile network. When a node in its mobile network wishes to send a packet out of the network, the mobile router intercepts the packet and forwards the packet to the home agent through the IP-in-IP tunnel. The home agent then sends the packet out to the intended recipient.

Another solution proposed in [Non-patent document 12] is an extension of Mobile Router Support [Non-patent document 11]. It involves the use of a Reverse Routing Header to avoid having too many levels of encapsulation when mobile network get nested (i.e. a mobile network attaching itself to another mobile network). Here, the lowest level mobile network sets up a Reverse Routing Header in its tunnel packet to its home agent. As high-level mobile routers intercept this tunnel packet on its way, the higher-level mobile router does not encapsulate this packet into another IP-in-IP tunnel. Instead, the high-level mobile router copies the so

source address in the packet to the Reverse Routing Header, and put its own care-of-address as the source address. In this way, when the home agent of the first mobile router receives the packet, it can determine the chain of mobile routers that is in the path between the first mobile router and itself. Subsequently when the home agent wishes to forward another intercepted packet for the first mobile router, it can include a Routing Header [Non-patent document 8] so that the packet is directly sent to the first mobile router via other high-level mobile routers.

A third solution for the network in motion problem is proposed in [Non-patent document 13], known as the Prefix Scope Binding Update. Here, the solution proposed to add to the Binding Update sent by mobile routers the information on the prefix of the mobile network. In this way, home agents can deduce that any nodes with a prefix equal to that specified in the Binding Updates are attached to the mobile router. Hence, the home agent can forward packets destined to these nodes to the mobile router.

Problems to be solved

In [Non-patent document 11], the use of IP-in-IP tunnelling suffers from what is known as route triangulation. This happens when a packet from one node to another node needs to pass through a third party (in this case, the home agent) that is not situated on the shortest path between the source and destination. The effect of route triangulation is compounded when mobile networks are nested. For example, consider a packet from a mobile network that needs to be forwarded through three mobile routers. Using the solution proposed in [Non-patent document 11], the packet will have to be encapsulated in three different tunnels, where each tunnel is directed to different home agents of the different mobile routers. Not only does this multiple tunnelling cause considerable delays to

o the delivery of the packet, it also increases the probability of the packet being fragmented en route, since encapsulation increases the overall packet size. Reassembly of fragmented packets introduces additional processing delays, and may result in the entire packet being discarded if one of the fragments gets lost on its way.

The solution proposed in [Non-patent document 12] attempts to solve this problem by avoiding multiple tunnels. In this solution, only the first mobile router needs to set up an IP-in-IP tunnel with its home agent.

Subsequent mobile routers will not further encapsulate the packet. Instead, these routers record the original source address in a Reverse Routing Header, change the source address to their own care-of-addresses, and forward the packet to its destination without going through their home agents. Although this solution solves the multiple tunnels problem in a very efficient manner, it is very difficult for home agents to verify that the list of addresses recorded in the Reverse Routing Header is authentic. It is crucial for the home agents to be able to establish that the addresses recorded in the Reverse Routing Header are legitimate, since [Non-patent document 12] requires that home agent to make use of the list of addresses in a Reverse Routing Header to construct a Routing Header to forward any packet directly to the mobile router. The solution in [Non-patent document 12] does not provide any remedies to the security threats a Reverse Routing Header is exposed to.

Another simple solution to solve the problem of multiple tunnelings is to allow subsequent mobile routers to forward the outer packets directly to their specified destination (instead of encapsulating them in an additional level of tunnelling through the home agents of the subsequent mobile routers). This, however, faces the same security problem, since the recipient cannot verify that the outermost packet came from legitimate sources.

Means for Solving the Problems

To solve the problem listed in section 3.3, the present invention employs a mechanism for mobile network elements to pass information to their home agents or other corresponding nodes about the access routers the mobile nodes are attached to. Using this information, home agents or corresponding nodes can construct a routing header to send packets directly to the mobile nodes without incurring additional penalties of route triangulations. Because information about the routers the mobile nodes attached to are passed by the mobile nodes themselves, the authenticity of the information is automatically established.

In addition, since the home agents or other corresponding nodes received information about the routers the mobile nodes attached to, they can verify that packets arriving from a tunnel with the outer source address to be one of the access routers came from legitimate sources. Thus, mobile routers can now directly forward outer packets directly to the specified destinations, since it is now possible for recipients to verify the authenticity of the forwarding routers.

Operation of the Invention

This invention involves the internetworking of packet-switched data networks. Some of these networks are moving, such that the router controlling the egress interfaces of the said network changes its point of attachment. This invention provides extension to existing solutions for provisioning of global connectivity to roaming hosts, so that global connectivity to roaming networks can also be achieved.

This invention disclosed several algorithms to be employed in three main types of nodes. These are the mobile hosts that change their points of attachment to the global data communications network, the mobile rout

ers that control the egress interfaces of moving networks, and other hosts on the global data communications network that communicates with mobile hosts and mobile routers. With these algorithms fully deployed, packets to and from moving networks can be delivered to their intended destinations with minimal latency.

Embodiments

A method for provisioning global connectivity to roaming network is disclosed in this section. To help understand the disclosed invention, the following definitions are used:

* A "packet" is a self-contained unit of data of any possible format that could be delivered on a data network. A "packet" normally consists of two portions: a "header" and a "payload" portion. The "payload" portion contains data that are to be delivered, and the "header" portion contains information to aid the delivery of the packet. A "header" must have a source address and a destination address to respectively identify the sender and recipient of the "packet".

* A "packet tunnelling" refers to a self-contained packet being encapsulated into another packet. The act of "packet tunnelling" is also referred to as "encapsulation" of packets. The packet that is being encapsulated is referred to as the "tunnelled packet" or "inner packet". The packet that encapsulates the "inner packet" is referred to as the "tunnelling packet" or "outer packet". Here, the entire "inner packet" forms the payload portion of the "outer packet".

* A "mobile node" is a network element that changes its point of attachment to the global data communications network. It may be used to refer

to an end-user terminal, or an intermediate network element that serves as a gateway, a router, or an intelligent network hub that can change its point of attachment to the global data communications network. The "mobile node" that is an end-user terminal is more specifically referred to as a "mobile host"; whereas the "mobile node" that is an intermediate network element that serves as a gateway, a router, or an intelligent network hub is more specifically referred to as a "mobile router".

* An "access router" of a mobile node is a network element that serves as a gateway, a router, or an intelligent network hub to which the said mobile node attaches in order to gain access to the global data communications network through the said network element.

* A "home-address" is a primary global address assigned to a mobile node that can be used to reach the mobile node regardless of where on the global data communications network the mobile node is currently attached to.

* A mobile node that is attached to the global data communications network where its home-address is topologically compatible with the addresses used in the vicinity of the point of attachment is referred to as "at home". The vicinity of this point of attachment that is controlled by a single administrative authority is referred to as the "home domain" of the mobile node.

* A mobile node that is attached to the global data communications network at a point where the home-address of the said mobile node is topologically incompatible with the addresses used in the vicinity of that point of attachment is referred to as "away", and the vicinity of the said po

int of attachment is referred to as the "foreign domain".

* A "care-of-address" is a temporary global address assigned to a mobile node that is away such that the assigned "care-of-address" is topologically compatible with the addresses used in the vicinity of the mobile node's point of attachment to the global data communications network. A "care-of-address" is typically only valid for the period of time when the mobile node is attached to the same access router.

* A "home agent" is a network entity that resides at the home domain of a mobile node that performs registration services of care-of-addresses of the mobile node when it is away, and to forward packets addressed to the home-address of the mobile node to the care-of-address of the mobile node.

* A "corresponding node" refers to any network element that is on the global data communications network to which a mobile node is communicating with.

* A "Binding Update" is a message sent from a mobile node to its home agent or a corresponding node that informs the recipient the current care-of-address of the sender. This forms a "binding" between the care-of-address and the home-address of the mobile node at the recipient.

* A "Binding Acknowledgement" is a message sent from a recipient of the Binding Update message to the sender of the said Binding Update message, indicating the results of the binding.

* A "routing header" refers to a piece of information that is attached t

o a packet that instructs intermediate routers in a global data communications network where the packet should be forwarded to. Ordinarily, routers in a global data communications network will forward packets based on the destination. A "routing header" overwrites that behaviour by containing a list of intermediate destinations. To use a "routing header", a sender puts the address of the intended recipient in the last entry of the routing header, and places the first intermediate destination in the destination address of the packet. The first destination, upon receiving the packet, will update the packet with the "routing header" such that the packet will then be forwarded to the second intermediate destination (i.e. the destination address of the packet is swapped with the next entry in the "routing header"). The cycle repeats until the last intermediate destination is reached, where the "routing header" is updated such that the packet is now forwarded to the actual intended destination. Readers are referred to [Non-patent document 8] for a more detailed explanation of the operation of a "routing header".

* Any network element that supports or implements the methods and mechanisms disclosed in this invention is referred to as an "invention-enabled" network element.

In the following description, for purpose of explanation, specific numbers, times, structures, and other parameters are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to anyone skilled in the art that the present invention may be practiced without these specific details.

In order for the disclosed invention to co-exist in a global data communications network that contains network elements which may not support methods and mechanisms disclosed in this invention, any invention-enable

d router must indicate that they are capable of using methods and mechanisms disclosed in this document. This may be accomplished by inserting a unique signal into messages that routers occasionally broadcast to their neighbours. Anyone skilled in the art should be able to recognize various existing methods where a network element can notify other network nodes their capabilities. In addition, it should also be possible for any mobile nodes that attached themselves to a network segment controlled by a mobile router to learn the home-address of the said mobile router via the specified broadcast messages from the said mobile router.

For example, in the context of Internet Protocol version 6 [Non-patent document 8], a Home-Address Option can be inserted into the Router Advertisement Message specified in IPv6 Neighbor Discovery [Non-patent document 14] sent by an invention-enabled router to advertise its home-addresses. The Home-Address Option should contain the following fields: (1) a type field to identify this option as the Home-Address Option, (2) a length field to indicate the size of this option, and (3) a home-address field to specify the home-address of the sender, as recited in claim 3.

From the broadcast message sent by invention-enabled routers, a mobile node can then include the home-address of the access router the mobile node attached to in Binding Updates sent by the mobile node, as recited in claim 1. This should be done only when the access router is invention-enabled. Such an information can be embedded in a Binding Update message in various possible different ways, depending on the underlying protocol the global data communications network used. For example, in the context of Internet Protocol version 6 [Non-patent document 8], an Access-Router-Address Option can be inserted into the Binding Update Message defined in Mobile IPv6 [Non-patent document 7]. Such an option should contain the following fields: (1) a type field to identify this option as the Access-Router-Address Option, (2) a length field to indicate the si

ze of this option, and (3) an access-router-address field to specify the home-address of the access router the send is attached to, as described in claim 2.

When an invention-enabled recipient, which may be the home agent of the mobile node or a corresponding node, received this Binding Update, the recipient can record this in a table or a list. Entries in such a table or list, hereafter referred to as Binding Entries, should at least contain the following three fields:

(1) a home-address field containing the home-address of mobile node; (2) a care-of-address containing the care-of-address of mobile node; and (3) an access-router-address field containing the home-address of access router, as recited in claim 5. The values of these three fields can be extracted from a Binding Update message.

Figure 1 illustrates the algorithm used to update the Binding Entries when an invention-enabled network element receives a Binding Update message, as recited in claim 6. In the step marked with literal 101, an entry is searched within the Binding Entries for which the home-address field equals to the home-address in the Binding Update message. If none is found, a new entry is created, as shown in the steps marked with literals 102 and 103. If the Binding Update message does not contain any care-of-address, or if the care-of-address equals to the home-address, it is assumed that the sender of the Binding Update has returned to its home domain, and thus the entry is deleted from the Binding Entries, as shown in the steps marked with literals 104, 105, and 106. Else, the care-of-address field in the entry is updated to the care-of-address specified in the Binding Update message, as shown in the step marked with literal 107. If the Binding Update message includes a home-address of access router, the access-router-address field in the entry is updated, as shown in the steps marked with literals 108 and 109. Otherwise, it is assumed

that the sender of the Binding Update is currently attached to an access router that is not invention-enabled. In this case, the access-router-address field is marked to be invalid, as shown in the step marked with literal 110.

A sender of the Binding Update can optionally request for a Binding Acknowledgement. This allows the recipient of the Binding Update to inform the sender the result of the update. When an invention-enabled recipient of a Binding Update that contains a valid access-router-address information replies with a Binding Acknowledgement, it should mark the Binding Acknowledgement in such a way that the recipient of the Binding Acknowledgement can deduce that the sender of the Binding Acknowledgement is invention-enabled, with reference to claim 4. It should be apparent to anyone skilled in the art that such a marking can be achieved in various ways, including, but not limited to, a bit flag or a specific pattern of a bit stream in the Binding Acknowledgement.

Using the Binding Entries, the corresponding node or home agent can construct a routing header to reach the mobile node directly. The routing header can be constructed such that the packet will be first forwarded to the access router's home-address, then to the care-of-address of the mobile node. In this way, the packet does not have to traverse to the home domain of the mobile node and get intercepted by the home agent who then forwards the packet to the mobile node at its care-of-address.

If the access router itself is mobile and away, the packet will still follow a roundabout route, even though a routing header is used. This is because since the access router is away, the packet forwarded to the home-address of the access router will be routed to the home domain of the access router. The home agent of the access router will intercept the packet, and forward it to access router at the care-of-address of the access router.

It may be possible to further optimise the delivery of packets by having the invention-enabled access router send Binding Update to the invention-enabled home agent and corresponding nodes of the mobile nodes. The access router should also attach the home-address of its own access router in the Binding Update if it is also invention-enabled. In order not to incur significant latency when the access router moves (if it is mobile), any invention-enabled mobile node should maintain a list of other hosts, both home agents and corresponding nodes, that it has sent a Binding Update. This list is hereafter referred to as the Bound Hosts List.

When a mobile node moves, it should notify the hosts on its Bound Host List by sending the respective hosts Binding Updates. However, to avoid introducing a burst of Binding Updates whenever a mobile node moves, there should be a small delay between subsequent transmissions of Binding Updates.

When invention-enabled mobile nodes and access routers notify the hosts with Binding Updates, any invention-enabled home agent or corresponding nodes can then gain sufficient knowledge of the network topology around a mobile node to optimise the delivery of packets to the mobile node.

To do so, the algorithm depicted in Figure 2 can be used when constructing routing header from the Binding Entries, as recited in claim 7.

In the algorithm, a stack (a last-in-first-out storage structure) is used to aid the construction of the routing header. In the step marked with literal 201, the stack is initialised to be empty. In addition, two temporary variables src and dst are set to the source (i.e. the home agent or corresponding node sending the packet) and destination addresses (i.e. the home-address of the mobile node) of the packet respectively, as shown in the step marked with literal 202. The algorithm then enters a loop of steps marked with literals 203 through 209. In the loop, the Binding Entries is searched for an entry with the home-address field equ

al to the value stored in dst. If none is found, the loop exits, as shown in the steps marked with literals 203 and 204. On the other hand, when an entry is found, the value in dst is checked to see if it is the home-address of the mobile node (which should be true only once at the first iteration of the loop). If so, the value in dst is pushed onto the stack, as shown in the steps marked with literals 204, 205, and 206.

The algorithm next updates the value in dst to store the care-of-address field in the binding entry found, as shown in the step marked with literal 207. The access-router-address field of the binding entry is then checked to see if it contains a valid address. If so, the loop is reiterated, as shown in the steps marked with literals 208 and 209. In the step 209, the content of the dst field is also pushed onto the stack. If the access-router-field is invalid, the loop is exited. Once out of the loop, the contents in the stack is popped out in reverse order and appended to the routing header, as shown in the steps marked in literal 210 and 211. Once the stack is emptied, the destination field of the packet is set to the value stored in dst and the algorithm finishes, as shown in the step marked with literal 212.

While the routing header so constructed can optimise the routing of a packet delivered to the mobile node, it also introduces certain security threats. The most notable threat is that an attacker can construct a specific routing header such that packets will be reflected from a node in a mobile network, so that the attacker can reach some parts of the global data communications network that are otherwise inaccessible. To avoid such a security breach, any invention-enabled mobile nodes should follow the algorithms depicted in Figures 3 and 4 to discard any packets that are suspected to be bogus.

The algorithm illustrated in Figure 3 is used by an invention-enabled router. When a packet is intercepted by the router, the router first ch

ecks if the destination address equals to its home-address or its care-of-address, as shown in the steps marked with literals 301 and 303. If the destination address equals to the home-address, the packet is consumed, as shown in the step marked with literal 302. If the destination address equals to the care-of-address, the presence of a routing header is checked, as shown in the step marked with literal 304. If the destination address is neither the home-address nor care-of-address, it is checked if it is a valid address in the local network attached to the router, as shown in the step marked with literal 305. If it is, the packet is forwarded to its destination, as shown in the step marked with literal 311. Otherwise, the packet is discarded, as shown in the step marked with literal 310.

In the step marked with literal 304, the presence of the routing header is checked. If none is present, the packet is discarded, as shown in the step marked with literal 310. Should a routing header exist, it is checked if the next address in the routing header is the last entry. If not, the entry is swapped with the destination address of the packet, and the destination address is again checked if it is a valid address in the local network attached to the router, as shown in the steps marked with literals 306, 307, 305. If the next address in the router header is the last entry, this last entry is checked to see if it is the home-address of the router, as shown in the steps marked with literals 306 and 308. If it is the home-address, the packet is consumed, as shown in the step marked with literal 309. Else, the packet is discarded, as shown in the step marked with literal 310.

For a mobile host (i.e. a mobile node that is not functioning as a router), the algorithm shown in Figure 4 is used. First, in the step marked with literal 401, the destination address is checked to see if it is the home-address of the mobile node. If yes, the packet is consumed, as

shown in the step marked with literal 406. Else, the destination address is checked to see if it is the care-of-address of the mobile node, as shown in the step marked with literal 402. If it is not, the packet is discarded, as shown in the step marked with literal 407. On the other hand, if the destination address equals the care-of-address of the mobile node, the presence of a routing header is checked. In addition, the routing header must contain only one remaining entry, and that entry must be the home-address of the mobile node, as shown in the series of verification steps marked with literal 403, 404, and 405. The packet is discarded if any of these tests fails, as shown in the step marked with literal 407. If all the tests pass, the packet is consumed as shown in the step marked with literal 406.

The above description fully explains how a packet can be delivered to the mobile node without going through the home agents of the mobile node and access router(s), thereby reducing delivery latency. The next part of the disclosure focuses on the packets sent from the mobile node. One point to note here is that when an away mobile node sends a packet, it usually uses its care-of-address as the source of the packet. This is done because in a lot of packet-switched network that is deployed, ingress filtering is used for security reasons. Ingress filtering refers to the discarding of packets going out of a local network because the discarded packets have source addresses that are topologically incompatible with the addresses used in the said local network. When an away mobile node uses its home-address as the source address to send a packet from within a foreign domain, the packet may be discarded due to ingress filtering. Thus, to avoid ingress filtering, the care-of-address (which is topologically compatible with the addresses used in the foreign domain) is used as the source address. To help the recipient identify the originator of the packet, the away mobile node will include its home-address in

the header of the packet. Hence, in summary, whenever an away mobile node sends a packet, it marks the source address of the packet with its care-of-address, and inserts its home-address as extra information in the packet header.

When the mobile node is aware that its access router is invention-enabled, it can choose to allow the access router to forward the packet it sent directly to the destination, without going through the packet tunneling between the access router and the home agent of the access router.

With reference to claim 8, this can be done by inserting a signal into the packet header. This signal can be of any form, such as a bit or a particular pattern of bit stream. The presence of such a signal indicates to an invention-enabled router that the sender of the packet is requesting the router to attempt to forward the packet directly to the destination without using any packet tunneling or encapsulation technology. Hereafter in the document, this signal is referred to as the "direct-forwarding-request". With reference to claim 9, an intermediate router can invalidate the direct-forwarding-request signal when it does not wish subsequent routers to attempt to forward the packet directly to the destination without using any packet tunnelling or encapsulation technology.

When an invention-enabled mobile router intercepts this packet and notices that the packet is specially marked with a direct-forwarding-request, it checks if the source address of the packet is a valid address from its local network. If it does not, this means that there exist at least one intermediate network element between the originator of this packet and the router itself that is not invention-enabled. In this case the router cannot perform direct forwarding. Next, it checks if it has a binding update with the specified destination. If so, it changes the source address to its care-of-address and sends the packet to the destination.

For any other case, the packet is encapsulated and tunnelled to the ho

me agent of the mobile router, where it is de-capsulated and delivered to the actual destination. This, of-course assumes that the mobile router itself is away from home. If it is at home, there is no need to check for direct-forwarding-request. Any packet it intercepts from its local network is by default forwarded to the destination without the need to tunnel the packet to a home agent.

With reference to claim 10, this is illustrated in the block diagrams shown in Figure 5. When an invention-enabled mobile router that is away from home intercepts a packet, it first checked if the packet is marked with a direct-forwarding-request, as shown in the step marked with literal 501. Next, the source address in the packet is verified to be a valid address in the mobile router's local network, as shown in the step marked with literal 502. Finally, the specified destination is checked to see if the mobile router has previously sent a Binding Update, as shown in the step marked with literal 503. If any of the three tests is negative, the packet is forwarded to the home agent using tunnelling, as shown in the step marked with literal 504. Otherwise, the packet is forwarded directly, as shown in the step marked with literal 505. Here the invention-enabled mobile router will modify the packet header so that the source address will be replaced by its care-of-address.

Since the source address of a packet is changed by routers en-route, there must be a way for recipient of the packet to verify that the packet originated from authentic source. The inclusion of the home-address of the mobile node sending the packet in the packet header provides one form of verification. However, an attacker can forge a packet and falsely insert the home-address information into the packet header. Thus, it is of great importance for recipient to establish that the source address on the packet received is an authorized invention-enabled access router of the sender (the sender here refers to the mobile node with the speci

fied home-address). One way to do so is to check through the Binding Entries, and established the fact that the source address of a received packet is linked to the home-address inserted into the packet header. With reference to claim 11, Figure 6 depicts an algorithm that establishes such a relationship.

The algorithm shown in Figure 6 returns the Boolean value TRUE when a relationship can be established, and returns the Boolean value FALSE otherwise. When the algorithm first starts, a variable temp is first initialised to store the home-address specified in the packet header, as shown in the step marked with literal 601. The algorithm then enters a loop (marked with literals 602 through 607) to scan through the Binding Entries. First, the value in temp is checked against the source address of the packet. If they are equal, the algorithm returns TRUE, as shown in the step marked with literal 602. Else, an entry in the Binding Entries with a home-address field equal to the value stored in temp is searched for, as shown in the step marked with literal 603. If none is found, the algorithm returns FALSE, as shown in the step marked with literal 604.

If one such entry is found, the source address of the packet is compared against the care-of-address field in the entry found, as shown in the step marked with literal 605. If the two are identical, a relationship is established and the algorithm returns TRUE. Else, the access-router-address field of the entry found is checked if it contains a valid entry, as shown in the step marked with literal 606. If the access-router-address field is invalid, the algorithm returns FALSE. Else, the address in the access-router-address field is stored in temp, and the loop is reiterated, as shown in the step marked with literal 607.

With reference to claim 18, a basic invention-enabled node needs to implement the Binding Entries, and the algorithm that updates the Binding Entries as shown in Figure 1 and recited in claim 6. In addition, it sh

ould be able to mark a Binding Acknowledgement with a special information that allow the recipient of the said Binding Acknowledgment to realize that the information on the home-address of access router in the corresponding Binding Update message is accepted, as recited in claim 4. Furthermore, for security concerns, the invention-enabled node needs to implement the algorithm that checks the source address of a received packet as described in Figure 6 and recited in claim 11. Lastly, to be able to optimise the delivery of packet to an invention-enabled mobile node, the basic invention-enabled node needs to implement the algorithm to construct the routing header as depicted in Figure 2 and recited in claim 7.

Hence, with reference to claims 12 and 13, an invention-enabled node, after a short period of time from the reception of a Binding Update message with attached information on the home-address of the access-router the sender of the Binding Update message is attached to, will start to forward packets to the said sender through the specified access router. This is meant that after the reception of the said Binding Update, certain packets sent out from the invention-enabled node will possess one of the following feature: (1) the said packet has the source address field set to the home-address of the access router, and is appended with a routing header containing only the care-of-address and home-address of the said sender of the Binding Update; or (2) the said packet has the source address field set to the home-address of the access router, and is appended with a routing header containing the care-of-address of the said sender of the Binding Update as the first entry.

Should the said access router has also sent a Binding Update containing its care-of-address to the same invention-enabled node, the packets sent out from the invention-enabled node will possess one the following features: (1) the said packet has the source address field set to the care-of-address of the access router, and is appended with a routing header

containing only the care-of-address and home-address of the said sender of the Binding Update; (2) the said packet has the source address field set to the care-of-address of the access router, and is appended with a routing header containing the care-of-address of the said sender of the Binding Update as the first entry; or (3) the said packet is appended with a routing header containing the care-of-addresses of the said sender of the Binding Update and the access router, where the care-of-address of the access router comes immediately before the care-of-address of the said sender of the Binding Update, as recited in claims 14, 15, and 16.

For an invention-enabled mobile node, with reference to claim 19, in addition to those functionalities described for a basic invention-enabled node, the functionality to insert a direct-forwarding-request in a packet, as recited in claim 8, and to insert the home-address of its access router in a Binding Update message, as recited in claim 1, must be implemented. If the mobile node is not serving as a mobile router, the algorithm to check incoming packets as illustrated in Figure 4 must also be implemented.

With reference to claim 20, an invention-enabled mobile router will have to implement, on top of those specified for an invention-enabled mobile node, the functionality to check packets from the local network (i.e. ingress interface of the said router) for a direct-forwarding-request signal; as described in Figure 5 and recited in claim 10. In addition, the router has to perform security check on packets arriving from the egress interface as described in Figure 3.

Hence, with reference to claim 17, an invention-enabled node, after receiving a packet from its ingress interface that contain a direct-forwarding request signal, may forward the packet simply by changing the source address of the said packet to its own care-of-address or home-address.

This happens when the access router's Bound Host List contains the hos

t specified in the destination field of the packet. If the specified destination is not in the Bound Host List, the invention-enabled router may then send a Binding Update message to the specified destination.

Effects of Invention

The invention allows hosts in an internetworking of packet-switched data networks to use existing solutions of provisioning global connectivity to mobile hosts and extends these solutions to provide global connectivity to networks that change their points of attachment. By using the methods disclosed in this document, packets to and from roving networks can be delivered to their intended destinations with minimal latency. Furthermore, by using the verification methods provided by the current invention, network elements can reduce the security threats they are exposed to.

4 Brief Description of Drawings

Figure 1: Updating the Binding Entries - This figure depicts the algorithm employed by network element to update the Binding Entries when the said network element received a Binding Update message;

Figure 2: Construction of a Routing Header - This figure shows the algorithm employed by network hosts when constructing routing header to deliver a packet directly to a mobile node. The Binding Entries is used to recursively obtain the care-of-addresses of the mobile node and its access routers. A stack is used to store these addresses, and when constructing the routing header, the addresses can be retrieved in reverse order;

Figure 3: Security Verification by a Router - This figure depicts the steps performed by a router when it intercepted a packet to be forwarded

d to one of the local networks attached to the router. This sequence of tests helps to reduce the vulnerability of the local network to security threats;

Figure 4: Security Verification by a Mobile Node - This figure illustrates the checks carried out by a mobile node when it receives a packet.

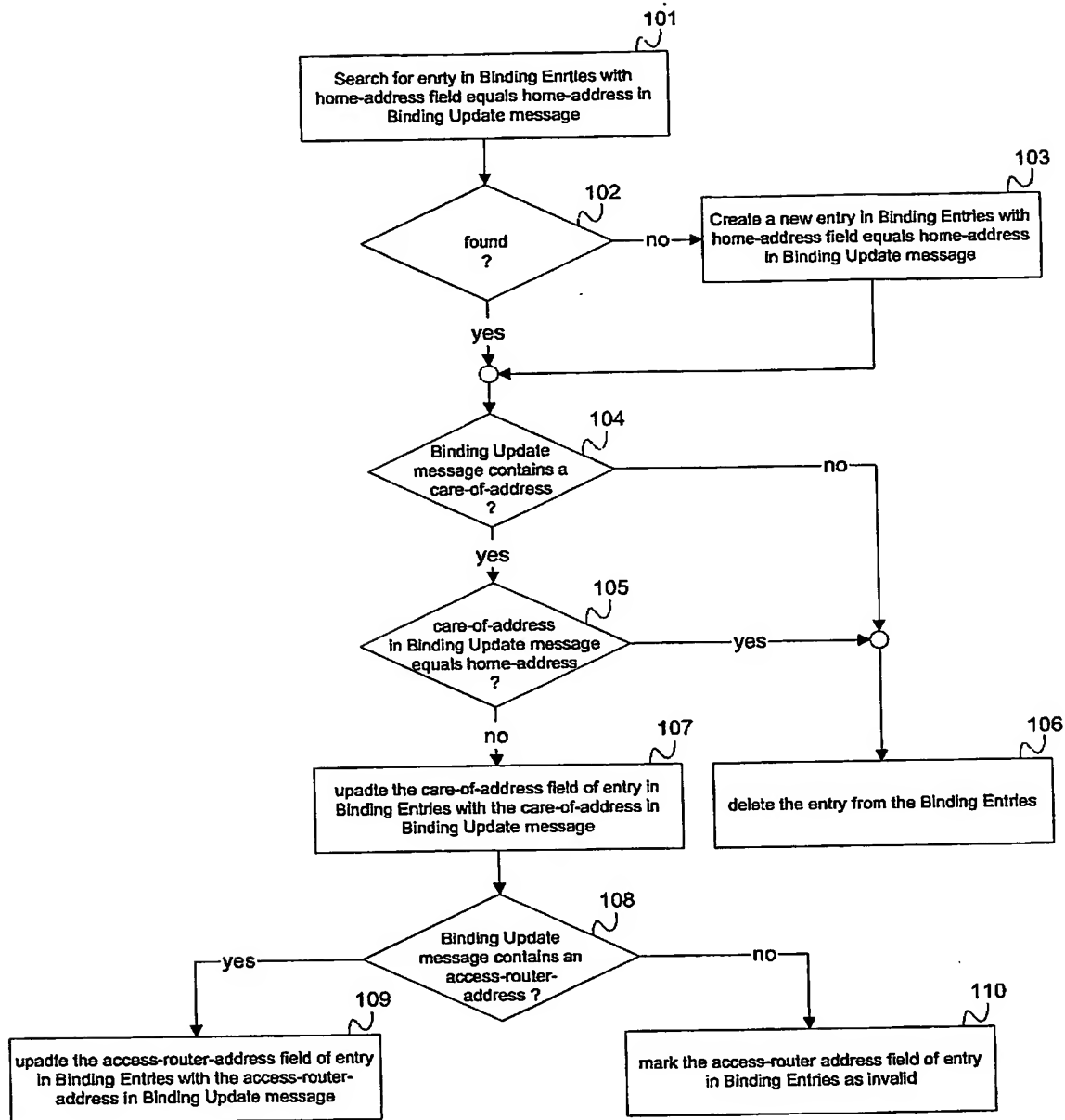
The verification process described here can reduce the vulnerability of the mobile node to security threats;

Figure 5: Handling of Direct Forwarding Request - This figure demonstrates the algorithm used by a router to process outgoing packets, i.e. packets sent by nodes in the local network attached to the router that are addressed to other hosts on the global data communications network;

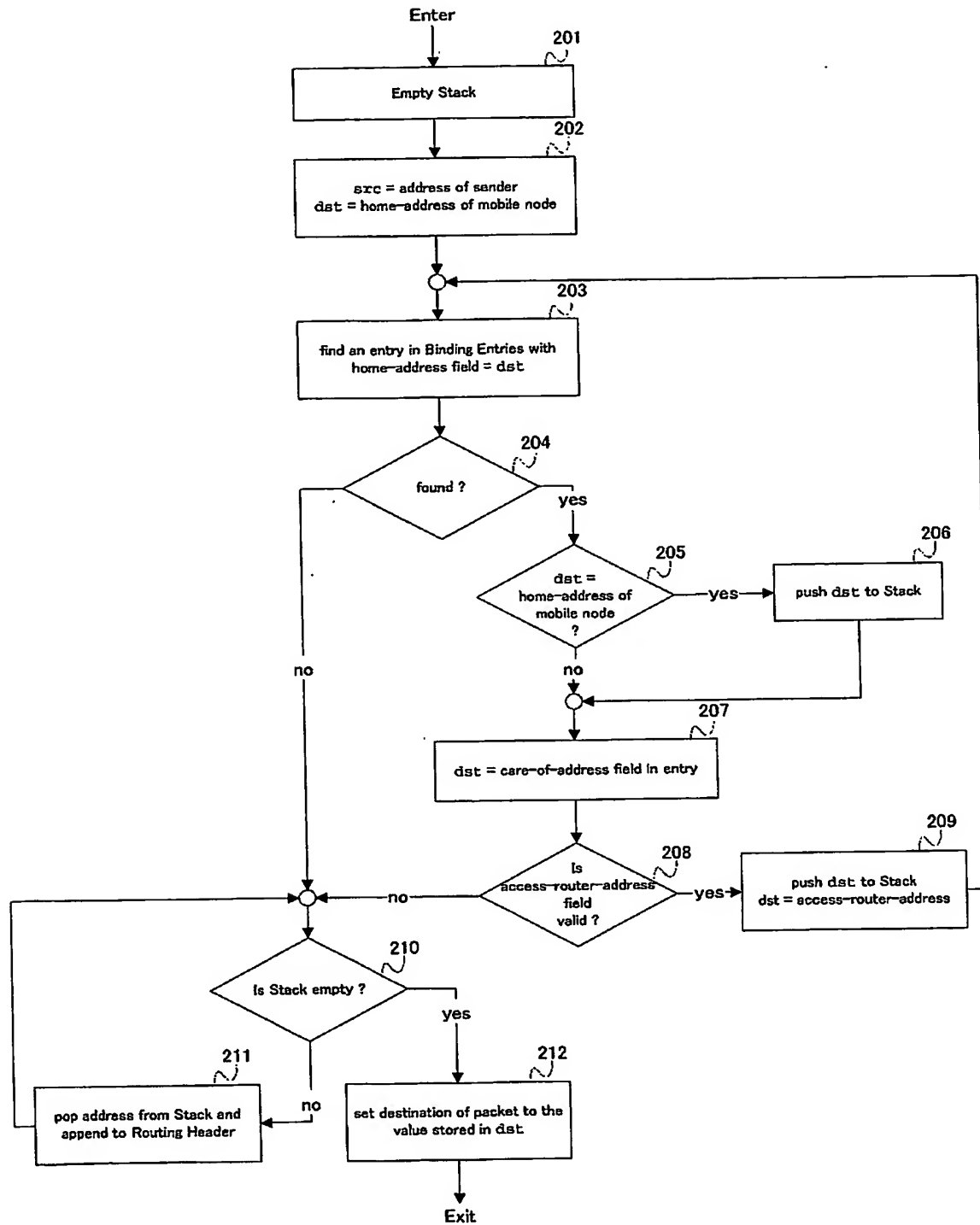
Figure 6: Security Verification by Other Hosts - This figure depicts the verification process used by network hosts, be it home agents or corresponding nodes, to check that a packet with a specified source address is linked to the home-address included in the packet header through previous Binding Updates. The algorithm shown in the figure basically scans through the Binding Entries iteratively to establish a relationship between the source address and home-address.

【書類名】 外国語図面

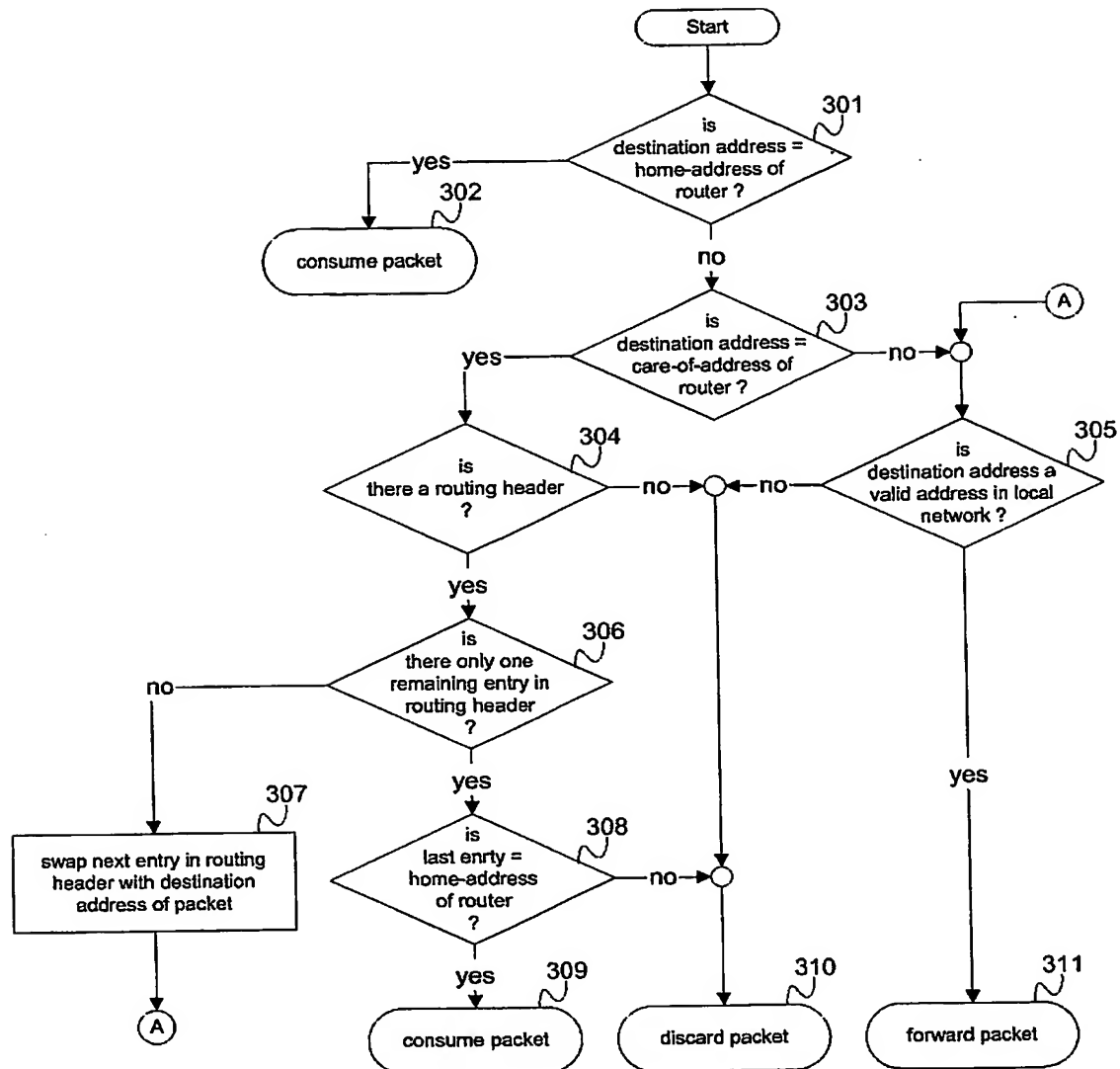
【図 1】



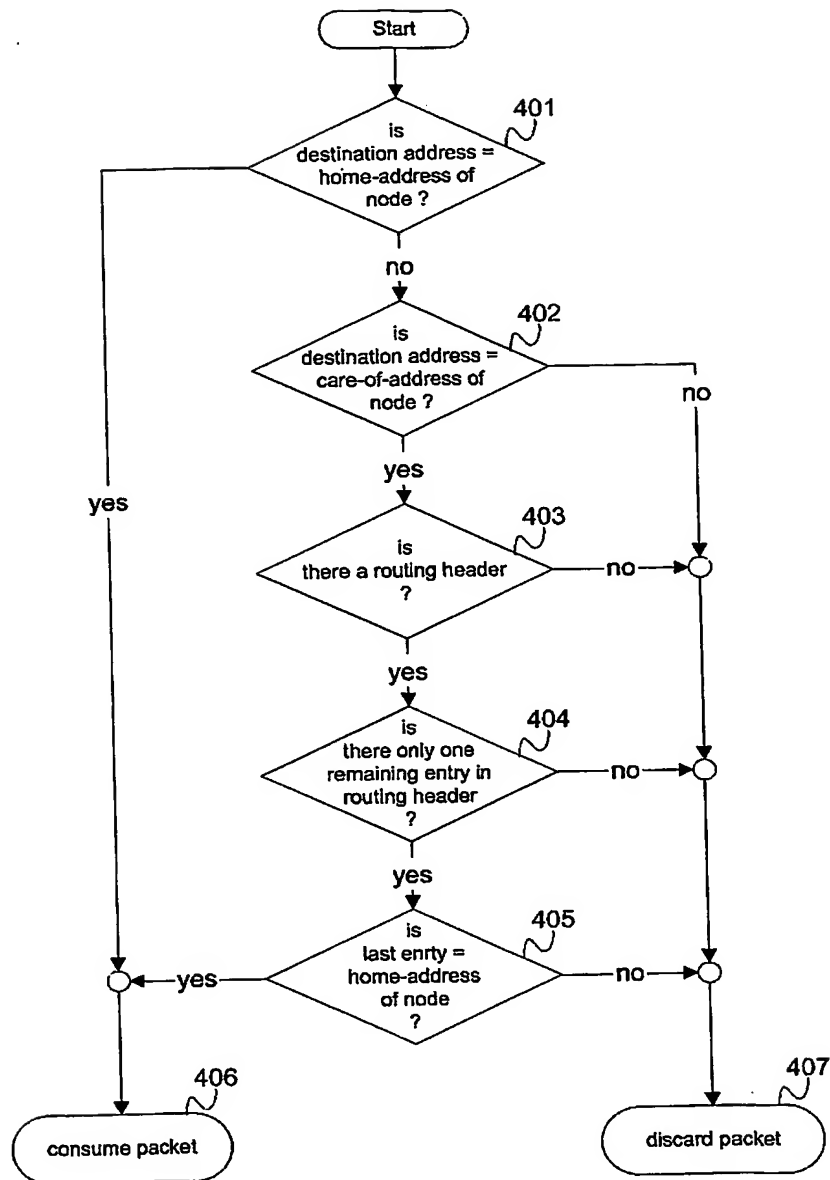
【図 2】



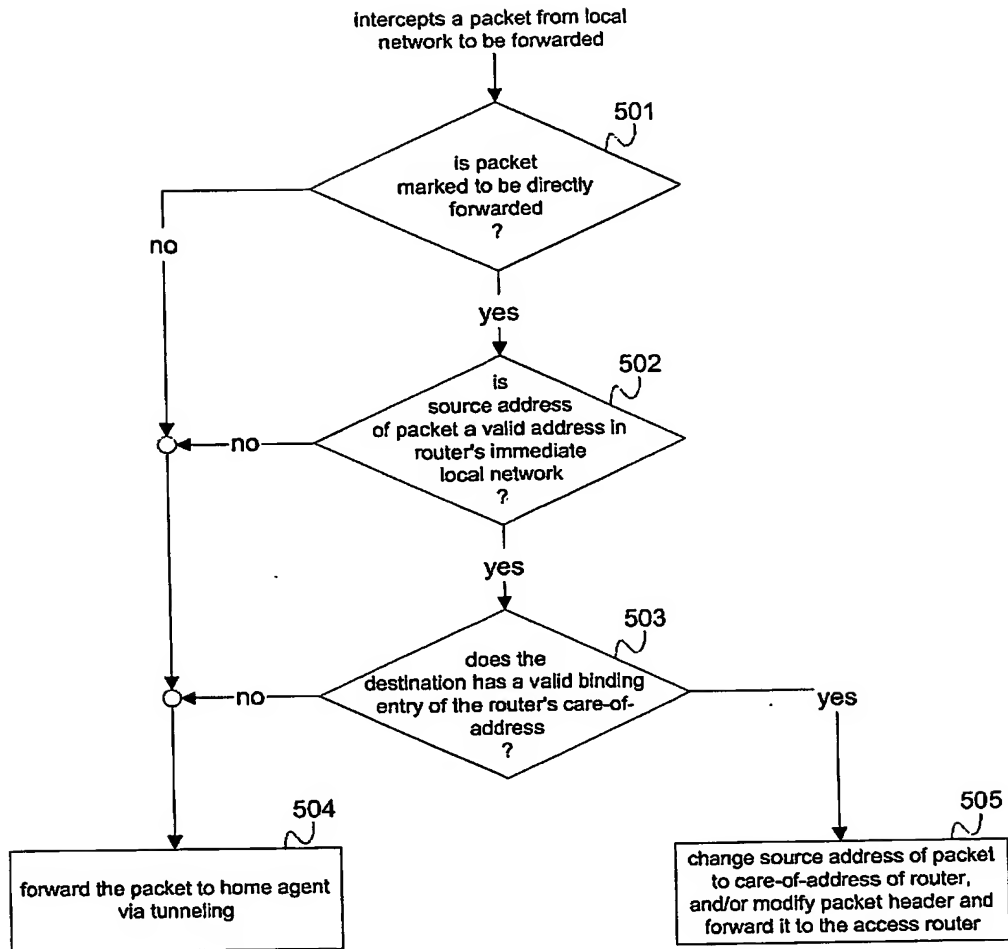
【図 3】



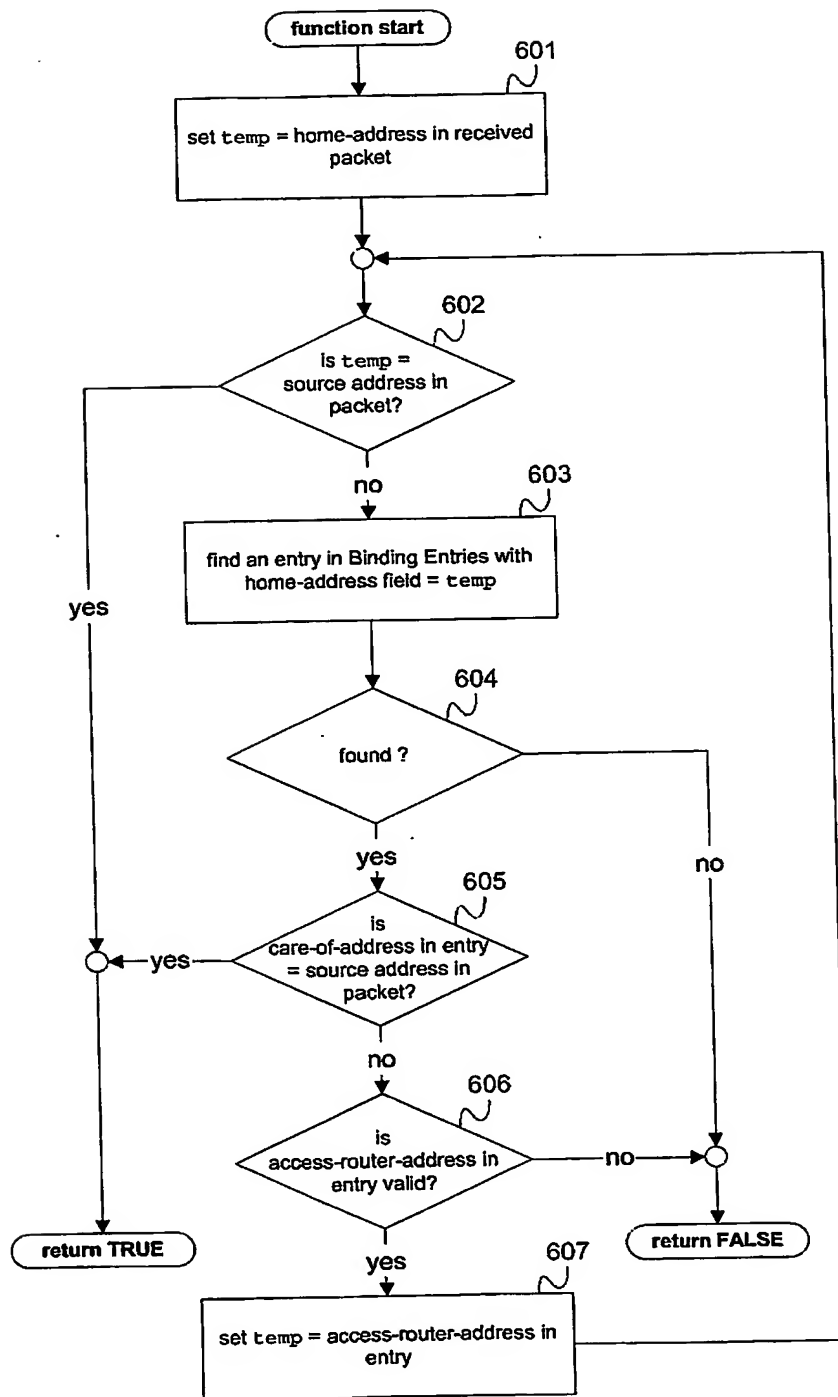
【図 4】



【図 5】



【図 6】



【書類名】 外国語要約書

1 ABSTRACT

An invention pertaining to the provisioning of global connectivity to networks that change their points of attachment is disclosed in this document. This invention provides several mechanisms and methods to be employed in different types of nodes in an internetworking of packet-switched data communications networks. The types of nodes are the mobile hosts that change their points of attachment to the global data communications network, the mobile routers that control the egress interfaces of moving networks, and other hosts on the global data communications network that communicates with mobile hosts and mobile routers. These algorithms and mechanisms are devised such that packets to and from moving networks can be delivered to their intended destinations with minimal delay. In addition, the current invention also introduces various mechanisms so that the security threats nodes employing methods disclosed in this invention are exposed to security threats are significantly reduced.

2 Representative Drawings Fig. 1

認定・付加情報

特許出願の番号

特願 2002-303879

受付番号

50201569277

書類名

特許願

担当官

小野寺 光子

1721

作成日

平成14年12月25日

<認定情報・付加情報>

【提出日】

平成14年10月18日

次頁無

【書類名】 翻訳文提出書

【整理番号】 2900645251

【あて先】 特許庁長官殿

【出願の表示】

【出願番号】 特願2002-303879

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100093067

【弁理士】

【氏名又は名称】 二瓶 正敬

【確認事項】

本書に添付した翻訳文は、特願2002-303879の正確な日本語への翻訳文であり、当該特許出願に記載されていない事項が本書に添付した翻訳文に記載されている場合には、当該出願が拒絶又は無効となる可能性がある」と承知していることを申し述べる。

【提出物件の目録】

【物件名】 外国語明細書の翻訳文 1

【物件名】 外国語図面の翻訳文 1

【物件名】 外国語要約書の翻訳文 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ローミング・ネットワークへのグローバル接続性を提供する方法及び装置

【特許請求の範囲】

【請求項 1】 パケット交換データ通信網のインターネットワーキングにおいて使用されるローミング・ネットワークへのグローバル接続性を提供する方法であって、前記通信網上のネットワーク・エレメントは主要なグローバル・アドレスによってユニークにアドレスが付けられ、それによって、前記ネットワーク・エレメントは前記通信網内のどこにローミングしようと到達可能となり、一方、前記ローミングするネットワーク・エレメントが単一のアクセス・ルータに接続されている期間は、前記通信網上でローミングする前記ネットワーク・エレメントに一時的なグローバル・アドレスが割り当てられ、それによって、前記ローミング・ネットワーク・エレメントは、グローバルなデータ通信網へのアクセスを獲得し、前記ローミング・ネットワーク・エレメントから単数又は複数の他のネットワーク・エレメントに対してバインディング・アップデート・メッセージを送るステップを有し、前記バインディング・アップデート・メッセージが、前記主要なグローバル・アドレスと前記送信するローミング・ネットワーク・エレメントの一時的なグローバル・アドレスとを含んで、前記受信するネットワーク・エレメントが前記記載されている一時的なグローバル・アドレスと前記記載されている主要なグローバル・アドレスとを関係付けられるようにし、さらに、前記ローミング・ネットワーク・エレメントが現在接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含んでいる方法。

【請求項 2】 前記パケット交換データ通信網の前記インターネットワーキングにおいて使用される前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 1 に記載の方法であって、前記パケット交換データ通信網の前記インターネットワーキングにおける前記ネットワーク・エレメントが、前記ローミング・ネットワーク・エレメントが接続されている前記アクセス・ルータの前記主要なグローバル・アドレスをバインディング・アップデート・メッセージに挿入するために、前記バインディング・アップデート・メッセージにデータ・

フォーマットを加え、前記データ・フォーマットが、

i. 前記データ・フォーマットが、前記送信者が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含むものであることを識別可能とするタイプ・フィールドと、

ii. 前記データ・フォーマットの長さを特定可能とするレンジス・フィールドと、

iii. 前記送信者が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含むアクセス・ルータ・アドレス・フィールドとを、
有する方法。

【請求項 3】 前記パケット交換データ通信網の前記インターネットワーキングにおいて使用される前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 1 に記載の方法であって、前記パケット交換データ通信網の前記インターネットワーキングにおける前記アクセス・ルータが、その主要なグローバル・アドレスをアドバタイズメント・メッセージに挿入するために、前記アドバタイズメント・メッセージにデータ・フォーマットを加え、前記データ・フォーマットが、

i. 前記データ・フォーマットが、前記送信者の前記主要なグローバル・アドレスを含むものであることを識別可能とするタイプ・フィールドと、

ii. 前記データ・フォーマットの長さを特定可能とするレンジス・フィールドと、

iii. 前記送信者の前記主要なグローバル・アドレスを含むアクセス・ルータ・アドレス・フィールドとを、
有する方法。

【請求項 4】 パケット交換データ通信網のインターネットワーキングにおける複数のネットワーク・エレメント間で使用されるローミング・ネットワークへのグローバル接続性を提供する方法であって、前記パケット交換通信網の前記インターネットワーキングで前記ネットワーク・エレメントのうちの 1 つがローミングしており、

i. 前記ローミング・ネットワーク・エレメントから別のネットワーク・

エレメントに対して、所定の主要なグローバル・アドレスと前記送信するローミング・ネットワーク・エレメントに付加的に割り当てられた一時的なグローバル・アドレスとを含んで、前記受信するネットワーク・エレメントが前記記載されている一時的なグローバル・アドレスと前記記載されている主要なグローバル・アドレスとを関係付けられるようにし、さらに、前記ローミング・ネットワーク・エレメントが現在接続されているアクセス・ルータの前記主要なグローバル・アドレスを含んでいる前記バインディング・アップデート・メッセージを送り、

i i. 前記バインディング・アップデート・メッセージの受信者から前記ローミング・ネットワーク・エレメントに対して、バインディング・アクノレッジ・メッセージを用いて返答し、前記バインディング・アップデート・メッセージは、前記バインディング・アップデート・メッセージの受理又は拒絶に関する情報を含み、さらに、前記バインディング・アップデート・メッセージ内に前記アクセス・ルータの前記主要なグローバル・アドレスを包含することに関して前記バインディング・アクノレジメント・メッセージの送信者が理解し適切な処置を講ずることができる旨を、前記バインディング・アップデートの受信者に通知する機能があることを示す情報を含む

ステップを有する方法。

【請求項5】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項1に記載の方法であり、ネットワーク・エンティティがバインディング・アップデート・メッセージを受けた場合、前記ネットワーク・エンティティがバインディング・エントリ内に前記バインディング・アップデート・メッセージを記録することができるものであって、前記バインディング・エントリが以下のフィールド；

i. 前記ローミング・ネットワーク・エレメントの前記主要なグローバル・アドレスを含むホーム・アドレス・フィールドと、

i i. 前記ローミング・ネットワーク・エレメントの前記一時的なグローバル・アドレスを含む気付アドレス・フィールドと、

i i i. 前記ローミング・ネットワーク・エレメントが接続される前記アクセス・ルータの前記主要なグローバル・アドレスを含むアクセス・ルータ・ア

ドレス・フィールドと、

により構成される方法。

【請求項 6】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 5 に記載の方法であって、前記ネットワーク・エンティティが前記バインディング・アップデート・メッセージを受けた場合、前記ネットワーク・エンティティがバインディング・エントリの更新を行い、

i. 前記バインディング・エントリが、前記受け取ったバインディング・アップデート・メッセージに記載されている前記主要なグローバル・アドレスに等しい前記ホーム・アドレス・フィールドを持ったエントリを含んでいるかどうかをチェックして、見つからない場合には新しいエントリを作成し、

ii. 前記バインディング・アップデート・メッセージが前記バインディング・アップデート・メッセージの前記送信者の前記一時的なグローバル・アドレスに関する情報を含まない場合には、前記受け取ったバインディング・アップデート・メッセージ内に記載されている前記主要なグローバル・アドレスに等しい前記ホーム・アドレス・フィールドを持つ前記バインディング・エントリ内の前記エントリを削除し、

iii. 前記一時的なグローバル・アドレスに関する情報が前記エントリ内のホーム・アドレス・フィールドに等しい前記バインディング・アップデート・メッセージに含まれる場合には、前記受け取ったバインディング・アップデート・メッセージ内に記載されている前記主要なグローバル・アドレスに等しい前記ホーム・アドレス・フィールドを持つ前記バインディング・エントリ内の前記エントリを削除し、

iv. 前記一時的なグローバル・アドレスが前記受け取ったバインディング・アップデート・メッセージに含まれており、その値が前記エントリ内の前記ホーム・アドレス・フィールドと同一ではない場合には、前記エントリの気付アドレス・フィールドを、前記受け取ったバインディング・アップデート・メッセージに記載されている前記一時的なグローバル・アドレスに設定し、

v. 存在する場合には、前記エントリの前記アクセス・ルータ・アドレス・フィールドを、前記バインディング・アップデート・メッセージ内に記載され

ている前記アクセス・ルータの前記主要なグローバル・アドレスに設定し、

v i. 受け取ったバインディング・アップデート・メッセージが前記アクセス・ルータの前記主要なグローバル・アドレスに関する情報を含まない場合には、前記エントリの前記アクセス・ルータ・アドレス・フィールドを無効に設定する

ステップを有する方法。

【請求項 7】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 5 に記載の方法であって、前記ネットワーク・エレメントが、データ・パケットに付加するルーティング・ヘッダの構築を行い、前記ルーティング・ヘッダは、前記パケット内に記載されている終点アドレスによって宛先が示される前記ネットワーク・エレメントに対して、別の目的地への転送を指示するために使用され、

i. 前記パケットの最終目的地の主要なグローバル・アドレスを格納するため、ラストイン・ファーストアウト・データ構造を空にして一時的な変数を初期化し、

i i. 前記バインディング・エントリ内において、そのエントリのホーム・アドレス・フィールドが、前述の一時的な変数内に格納された同一のアドレスを含んでいる前記エントリを探し出し、

i i i. 前記バインディング・エントリ内に前記エントリが見つかり、前記一時的なグローバル・アドレスの前記値が、前記パケットの前記最終目的地の前記主要なグローバル・アドレスと等しい場合には、前記ラストイン・ファーストアウト・データ構造の上段に前記一時的な変数の値を格納し、

i v. 前記バインディング・エントリ内に前記エントリが見つかった場合には、前記一時的な変数内の前記エントリの前記気付アドレス・フィールドに含まれる前記値を格納し、

v. 前記バインディング・エントリ内に前記エントリが見つかった場合には、前記ラストイン・ファーストアウト・データ構造の上段に前記一時的な変数の値を格納し、その後、前記一時的な値に前記エントリの前記アクセス・ルータ・アドレス・フィールド内の前記値を格納し、

v i . 前記エントリの前記アクセス・ルータ・アドレス・フィールドが有効な場合には、前記ステップ (i i)、(i i i)、(i v)、(v i) を繰り返し、

v i i . 前記バインディング・エントリ内の前記エントリが見つかるか、又は、前記見つかったエントリの前記アクセス・ルータ・アドレス・フィールドが有効ではない場合には、ラストイン・ファーストアウト・データ構造が空になるまで、ラストイン・ファーストアウト・データ構造内の上段の値を削除して、前記削除された値を前記データ・パケットに添えられたルーティング・ヘッダに付加することを繰り返し行い、

v i i i . 前記データ・パケットの前記終点アドレスに前記一時的な変数内に格納された前記値を設定する

ステップを有する方法。

【請求項 8】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 1 に記載の方法であって、データ・パケットに記載されている前記目的地に対して、前記ネットワーク・エレメントが前記データ・パケットを直接転送できるよう、前記ネットワーク・エレメントが接続されている前記アクセス・ルータに対して要求を行うため、前記データ・パケット上にユニークな信号を挿入するステップをさらに有する方法。

【請求項 9】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 1 に記載の方法であって、データ・パケットに記載されている前記目的地に対して、前記連続的な中間ルータが前記データ・パケットを直接転送しないよう、請求項 8 で明確となる前記データ・パケット上の前記ユニークな信号を無効化するステップを有する方法。

【請求項 10】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 8 に記載の方法であって、パケット交換データ通信網の前記インターネットワーキングにおける中間ネットワーク・エレメントがその内部ネットワーク側インターフェイスから受けたデータ・パケットの処理を行い、前記中間ネットワーク・エレメントが、その内部ネットワーク側インターフェイスの単数又は複数のローカル・データ通信網と、その外部ネットワーク側インターフェイ

スのパケット交換データ通信網の前記インターネットワーキングとの架橋となるルータとして機能し、

i. 前記中間ネットワーク・エレメントがパケット交換データ通信網の前記インターネットワーキングにおいてローミングを行わない場合には、前記受信パケットを転送し、

i i. パケット交換データ通信網の前記インターネットワーキングにおける特定のネットワーク・エレメントに対して送信するため、前記受信パケットを別の新しく作成されたパケットでカプセル化して、ここで、前記中間ネットワーク・エレメントがパケット交換データ通信網の前記インターネットワーキングにおいてローミングし、前記一時的なグローバル・アドレスが割り当てられている場合に、前記受信パケットがユニークな信号を含まないか、又は、前記ユニークな信号が無効化されているならば、前記特定のネットワーク・エレメントは前記新しく作成されたパケットから前記元のデータ・パケットを抽出して前記目的地に転送することとなり、

i i i. パケット交換データ通信網の前記インターネットワーキングにおける特定のネットワーク・エレメントに対して送信するため、前記受信パケットを別の新しく作成されたパケットでカプセル化して、ここで、前記中間ネットワーク・エレメントがパケット交換データ通信網の前記インターネットワーキングにおいてローミングし、前記一時的なグローバル・アドレスが割り当てられている場合に、前記受信パケットに記載されているソース・アドレスが、前記中間ネットワーク・エレメントの内部ネットワーク側インターフェイスの前記ローカル・ネットワークにおける有効なアドレスではないならば、前記特定のネットワーク・エレメントは前記新しく作成されたパケットから前記元のデータ・パケットを抽出して前記目的地に転送することとなり、

i v. パケット交換データ通信網の前記インターネットワーキングにおける特定のネットワーク・エレメントに対して送信するため、前記受信パケットを別の新しく作成されたパケットでカプセル化して、ここで、前記中間ネットワーク・エレメントがパケット交換データ通信網の前記インターネットワーキングにおいてローミングし、前記一時的なグローバル・アドレスが割り当てられている

場合に、前記中間ネットワーク・エレメントによる前記バインディング・アップデート・メッセージで、前記受信パケットに記載されている終点アドレスが送られておらず、前記バインディング・アップデート・メッセージが前記中間ネットワーク・エレメントの前記主要なグローバル・アドレス及び前記現在の一時的なグローバル・アドレスを含んでいるならば、前記特定のネットワーク・エレメントは前記新しく作成されたパケットから前記元のデータ・パケットを抽出して前記目的地に転送することとなり、

v. 前記中間ネットワーク・エレメントがパケット交換データ通信網の前記インターネットワーキングにおいてローミングし、前記一時的なグローバル・アドレスが割り当てられている場合に、前記受信パケットが前記ユニークな信号を含み、前記受信パケットに記載されている前記ソース・アドレスが前記中間ネットワーク・エレメントの前記内部ネットワーク側インターフェイスの前記ローカル・ネットワークで有効なアドレスであり、前記受信パケットに記載されている前記終点アドレスが前もって前記中間ネットワーク・エレメントによる前記バインディング・アップデート・メッセージであって、前記中間ネットワーク・エレメントの前記主要なグローバル・アドレス及び前記現在の一時的なグローバル・アドレスを含む前記バインディング・アップデート・メッセージで送られているならば、前記受信パケットの前記ソース・アドレスを前記中間ネットワーク・エレメントの一時的なグローバル・アドレスに変更し、その後、前記記載されている目的地に前記受信パケットを転送する

ステップを有する方法。

【請求項 11】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 5 に記載の方法であって、パケット交換データ通信網の前記インターネットワーキングにおける中間ネットワーク・エレメントが、前記ネットワーク・エレメントに宛てられた受信パケットに記載されているソース・アドレスが正当なものかどうかの確認を行い、前記受信パケットの送信者が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスであって、前記受信データ・パケットに記載されている前記ソース・アドレスとは異なるアドレスに関する情報が前記受信データ・パケットに含まれており、

i. 前記受信データ・パケットに含まれている前記主要なグローバル・アドレスを格納するために一時的な変数を初期化し、

ii. 前記一時的な変数に格納された前記値が前記データ・パケットに記載されている前記ソース・アドレスと等しい場合には、前記ソース・アドレスが正当なものであると宣言し、

iii. 前記一時的な変数に格納された前記値が前記データ・パケットに記載されている前記ソース・アドレスと等しくない場合に、前記一時的な変数に格納された前記値と等しい前記値を前記ホーム・アドレス・フィールド内に持つ前記バインディング・エントリ内のエントリを検索し、

iv. 前記一時的な変数に格納された前記値が前記データ・パケットに記載されている前記ソース・アドレスと等しくない場合に、前記一時的な変数に格納された前記値と等しい前記値を前記ホーム・アドレス・フィールド内に持つ前記バインディング・エントリ内のエントリが見つからないならば、前記ソース・アドレスが不当なものであると宣言し、

v. 前記バインディング・エントリ内のエントリが見つかった場合には、前記バインディング・エントリ内のエントリの気付アドレス・フィールドが、前記データ・パケットに記載されている前記ソース・アドレスに等しい値を含んでいるならば、前記ソース・アドレスが正当なものであると宣言し、

vi. 前記バインディング・エントリ内のエントリが見つかり、前記エントリの前記気付アドレス・フィールドが、前記データ・パケットに記載されている前記ソース・アドレスと等しくない値を含む場合には、前記エントリの前記アクセス・ルータ・アドレス・フィールドは無効ならば、前記ソース・アドレスが不当なものであると宣言し、

vii. 前記バインディング・エントリ内のエントリが見つかり、前記エントリの前記気付アドレス・フィールドが、前記データ・パケットに記載されている前記ソース・アドレスと等しくない値を含む場合には、前記エントリの前記アクセス・ルータ・アドレス・フィールドに含まれる内容を前記一時的な変数に格納し、

viii. 前記エントリの前記アクセス・ルータ・アドレス・フィールド

が有効である場合には、ステップ (i i i)、(i v)、(v)、(v i)、(v i i) を繰り返す

ステップを有する方法。

【請求項 12】 ルーティング・ヘッダを含むデータ・パケットを送るために、前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 1 に記載の方法であり、前記バインディング・アップデート・メッセージの送信者が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含む前記バインディング・アップデート・メッセージの受理が成功した後に使用される方法であって、

i. 前記データ・パケットの前記ソース・アドレスが、前記アクセス・ルータの前記主要なグローバル・アドレスとなるよう設定し、

i i. 前記ルーティング・ヘッダが、前記バインディング・アップデート・メッセージの前記送信者の前記一時的なグローバル・アドレス及び主要なグローバル・アドレスのみを含むよう設定する

ステップを有する方法。

【請求項 13】 ルーティング・ヘッダを含むデータ・パケットを送るために、前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 1 に記載の方法であり、前記バインディング・アップデート・メッセージの送信者が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含む前記バインディング・アップデート・メッセージの受理が成功した後に使用される方法であって、

i. 前記データ・パケットの前記ソース・アドレスが、前記アクセス・ルータの前記主要なグローバル・アドレスとなるよう設定し、

i i. 前記ルーティング・ヘッダが、最初のエントリとして、前記バインディング・アップデート・メッセージの前記送信者の前記一時的なグローバル・アドレスを含むよう設定する

ステップを有する方法。

【請求項 14】 ルーティング・ヘッダを含むデータ・パケットを送るために、前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項 1

に記載の方法であり、前記バインディング・アップデート・メッセージの送信者が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含む第1のバインディング・アップデート・メッセージの受理が成功した後、及び、前記アクセス・ルータによって送信され、前記アクセス・ルータの前記一時的なグローバル・アドレスを含む第2のバインディング・アップデート・メッセージの受理が成功した後に使用される方法であって、

i. 前記データ・パケットの前記ソース・アドレスが、前記アクセス・ルータの前記主要なグローバル・アドレスとなるよう設定し、

ii. 前記ルーティング・ヘッダが、前記第1のバインディング・アップデート・メッセージの前記送信者の前記一時的なグローバル・アドレス及び主要なグローバル・アドレスのみを含むよう設定する

ステップを有する方法。

【請求項15】 ルーティング・ヘッダを含むデータ・パケットを送るために、前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項1に記載の方法であり、前記バインディング・アップデート・メッセージの送信者が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含む第1のバインディング・アップデート・メッセージの受理が成功した後、及び、前記アクセス・ルータによって送信され、前記アクセス・ルータの前記一時的なグローバル・アドレスを含む第2のバインディング・アップデート・メッセージの受理が成功した後に使用される方法であって、

i. 前記データ・パケットの前記ソース・アドレスが、前記アクセス・ルータの前記一時的なグローバル・アドレスとなるよう設定し、

ii. 前記ルーティング・ヘッダが、最初のエントリとして、前記第1のバインディング・アップデート・メッセージの前記送信者の前記一時的なグローバル・アドレスを含むよう設定する

ステップを有する方法。

【請求項16】 ルーティング・ヘッダを含むデータ・パケットを送るために、前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項1に記載の方法であり、前記バインディング・アップデート・メッセージの送信者

が接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを含む第1のバインディング・アップデート・メッセージの受理が成功した後、及び、前記アクセス・ルータによって送信され、前記アクセス・ルータの前記一時的なグローバル・アドレスを含む第2のバインディング・アップデート・メッセージの受理が成功した後に使用される方法であって、前記ルーティング・ヘッダが、最初のエントリとして、前記第1のバインディング・アップデート・メッセージの前記送信者の前記一時的なグローバル・アドレスと、前記アクセス・ルータの前記一時的なグローバル・アドレスとを含み、前記ルーティング・ヘッダ内で前記第1のバインディング・アップデート・メッセージの前記送信者の前記一時的なグローバル・アドレスの直前に、前記アクセス・ルータの前記一時的なアドレスが現れるよう設定するステップを有する方法。

【請求項17】 前記ローミング・ネットワークへの前記グローバル接続性を提供する請求項8に記載の方法であって、前記ネットワーク・エレメントが、通信網の前記インターネットワーキングにおいてローミングし、その内部ネットワーク側インターフェイスの単数又は複数のローカル・データ通信網と、その外部ネットワーク側出力インターフェイスの packets 交換データ通信網の前記インターネットワーキングとの架橋となるルータとして機能し、その内部ネットワーク側インターフェイスから前記ユニークな信号を含む前記データ・パケットを受け取った後、

i. 前記データ・パケットのソース・アドレスをその一時的なグローバル・アドレスに変更し、

ii. その外部ネットワーク側インターフェイスに前記データ・パケットを転送する

ステップを有する方法。

【請求項18】 請求項1で明確となる packets 交換データ通信網のインターネットワーキングにおいて使用されるネットワーク・エレメントで使用される装置であって、以下の

i. 前記バインディング・エントリを使用する請求項5で明確となる方法

i i. バインディング・エントリを更新する請求項 6 で明確となる方法、
i i i. バインディング・アクノレジメントメッセージに指示を挿入し、
このような指示の存在によって、前記バインディング・アクノレジメント・
メッセージの前記受信者に対して、前記送信者が理解でき、前記バインディング
・アップデート・メッセージに前記アクセス・ルータの主要なグローバル・アド
レスを含ませる適切な処置を講ずることができる旨を通知することが可能となる
請求項 4 で明確となる方法、

i v. データ・パケットの前記ソース・アドレスをチェックする請求項 8
で明確となる方法、

v. ルーティング・ヘッダを構築する請求項 7、13、14、15、16
のいずれか 1 つで明確となる方法、

を実現するための手段を有する装置。

【請求項 19】 請求項 1 で明確となるパケット交換データ通信網のインター
ネットワーキングにおいて使用されるネットワーク・エレメントで使用される装
置であって、前記ネットワーク・エレメントが通信網の前記インターネットワー
キングにおいてローミングしており、以下の

i. 前記バインディング・エントリを使用する請求項 5 で明確となる方法、

i i. 前記バインディング・エントリを更新する請求項 6 で明確となる方
法、

i i i. バインディング・アクノレジメントメッセージに指示を挿入し、
この指示の存在によって、前記バインディング・アクノレジメント・メッセ
ージの前記受信者に対して、前記送信者が理解でき、前記バインディング・アッ
プデート・メッセージに前記アクセス・ルータの主要なグローバル・アドレスを
含ませる適切な処置を講ずることができる旨を通知することが可能となる請求項
4 で明確となる方法、

i v. データ・パケットの前記ソース・アドレスをチェックする請求項 1
1 で明確となる方法、

v. ルーティング・ヘッダを構築する請求項 7 で明確となる方法、

v i . 前記ネットワーク・エレメントが接続されている前記アクセス・ルータに対して、データ・パケットに記載されている目的地に前記データ・パケットを直接転送するよう要求する信号を前記データ・パケットに挿入する請求項 8 で明確となる方法、

v i i . 前記バインディング・アップデート・メッセージ内に、前記ネットワーク・エレメントが接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを挿入する請求項 1 及び 2 で明確となる方法、

を実現するための手段を有する装置。

【請求項 20】 請求項 1 で明確となるパケット交換データ通信網のインターネットワーキングにおいて使用されるネットワーク・エレメントで使用される装置であって、前記ネットワーク・エレメントが通信網の前記インターネットワーキングにおいてローミングしており、その内部ネットワーク側インターフェイスの単数又は複数のローカル・データ通信網と、その外部ネットワーク側インターフェイスのパケット交換データ通信網の前記インターネットワーキングとの架橋となるルータとして機能し、以下の、

i . アドバタイズメント・メッセージに前記ネットワーク・エレメントの前記主要なグローバル・アドレスの情報を加える請求項 3 で明確となる方法、

i i . 前記バインディング・エントリを使用する請求項 5 で明確となる方法、

i i i . 前記バインディング・エントリを更新する請求項 6 で明確となる方法、

i v . バインディング・アクノレジメントメッセージに指示を挿入し、このような指示の存在によって、前記バインディング・アクノレジメント・メッセージの前記受信者に対して、前記送信者が理解でき、前記バインディング・アップデート・メッセージに前記アクセス・ルータの主要なグローバル・アドレスを含ませる適切な処置を講ずることができる旨を通知することが可能となる請求項 4 で明確となる方法、

v . データ・パケットの前記ソース・アドレスをチェックする請求項 11 で明確となる方法、

v i . ルーティング・ヘッダを構築する請求項 7 で明確となる方法、

v i i . 前記ネットワーク・エレメントが接続されている前記アクセス・ルータに対して、データ・パケットに記載されている目的地に前記データ・パケットを直接転送するよう要求する信号を前記データ・パケットに挿入する請求項 8 で明確となる方法、

v i i i . 前記バインディング・アップデート・メッセージ内に、前記ネットワーク・エレメントが接続されている前記アクセス・ルータの前記主要なグローバル・アドレスを挿入する請求項 1 及び 2 で明確となる方法、

i x . 前記ネットワーク・エレメントの前記内部ネットワーク側インターフェイスから到着するデータ・パケットを処理し、前記ネットワークの前記外部ネットワーク側インターフェイスに転送する請求項 10 及び 17 で明確となる方法、

を実現するための手段を有する装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、パケット交換データ通信網のインターネットワーキングにおけるパケットの伝送に関する。特に、開示される発明は示された発明は、グローバルなデータ通信網に接するポイントを定期的に変えるノードに、ネットワークへの接続性を供給する際の問題に取り組んだものである。また、本発明は、ローミング・ホストへのグローバル接続性を提供するための既存の解決策の増強と見なすことも可能である。

【0002】

【従来の技術】

従来技術の文献に関する情報の開示

【非特許文献 1】

Soliman, H., and Pettersson, M., 「モバイル・ネットワーク (M O N E T) 問題の提示と対象範囲」、インターネット・ドラフト: draft-soliman-monet-statement-00.txt、2002 年 2 月、ワーク・イン・プログレス

【非特許文献2】

Ernst, T., and Lach, H., 「ネットワーク・モビリティ・サポート
要求条件」、インターネット・ドラフト: draft-ernst-monet-requirements-00.
txt、2002年2月、ワーク・イン・プロGRESS

【非特許文献3】

Lach, H. et. al., 「モバイル・ネットワーク・シナリオ、対象範囲
と要求条件」インターネット・ドラフト: draft-lach-monet-requirements-00.t
xt、2002年2月、ワーク・イン・プロGRESS

【非特許文献4】

Kniventon, T. J., and Yegin, A. E., 「モバイル・ネットワーク・
ワーキンググループのための問題の対象範囲及び要求条件」、インターネット・
ドラフト: draft-lach-monet-requirements-00.txt、2002年2月、ワーク・
イン・プロGRESS

【非特許文献5】

Perkins, C. E. et. al., 「IPモビリティ・サポート」、IETF RCF
2002、1996年10月

【非特許文献6】

DARPA, 「インターネット・プロトコル」、IETF RFC 791、1981
年9月

【非特許文献7】

Johnson, D. B., Perkins, C. E., and Arkko, J., 「IPv6にお
けるモビリティ・サポート」、インターネット・ドラフト: draft-ietf-mobilei
p-ipv6-18.txt、ワーク・イン・プロGRESS、2002年6月

【非特許文献8】

Deering, S., and Hinden, R., 「インターネット・プロトコル・バ
ージョン6 (IPv6) の詳細」IETF RFC 2460、1998年12月

【非特許文献9】

Simpson, W., 「IP-in-IPトンネリング」IETF RFC 1853、1995年
10月

【非特許文献 10】

Conta, A., and Deering, S., 「IPv6 における一般的なパケット・トンネリング」 IETF RFC 2473、1998 年 12 月

【非特許文献 11】

Kniveton, T., 「モバイル IP を備えたモバイル・ルータ・サポート」、インターネット・ドラフト: draft-kniveton-mobrttr-01.txt、ワーク・イン・プロGRESS、2002 年 3 月

【非特許文献 12】

Thubert, P., and Molteni, M., 「IPv6 リバース・ルーティング・ヘッダ及びモバイル・ネットワークへの適用」、インターネット・ドラフト: draft-thubert-nemo-reverse-routing header-00.txt、ワーク・イン・プロGRESS、2002 年 6 月

【非特許文献 13】

Ernst, T., Castelluccia, C., Bellier, L., Lach, H., and Oliver eau, A., 「モバイル IPv6 におけるモバイル・ネットワーク・サポート (プレフィックス・スコープ・バインディング・アップデート)、インターネット・ドラフト: draft-ernst-mobileip-v6-network-03.txt、2002 年 3 月

【非特許文献 14】

Narten, T., Nordmark, E., and Simpson, W., 「IPv6 のための近隣探索」 IETF RFC 2461、1998 年 12 月

【0003】

今日のインターネットは、固定ネットワーク・ノードのシステムの周辺で、多数のデータ通信網が展開する段階に発展している。これらの周辺ネットワークは、エッジ・ネットワークとして適切に知られており、一方、エッジ・ネットワークによって囲まれた固定ネットワーク・ノードのシステムは、コア (core) として知られている。無線技術の出現及び拡張で、これらのエッジ・ネットワークは、ますます無線の解決策に用いられ、モバイル・ネットワークと呼ばれる特別なエッジ・ネットワーク、又は、移動中のネットワーク (非特許文献 1、2、3、4) を形成している。

【0004】

本質的には、モバイル・ネットワークは、ネットワーク全体がインターネットへの接続点を変更するノードのネットワークであり、通常、異なるアクセス・ルータ（実際には、アクセス・ルータ自身が移動可能かもしれない）間でインターネットへの接続点を変更する、モバイル・ネットワーク内のモバイル・ルータ（モバイル・ネットワークをインターネットにつなぐもの）を必要とする。モバイル・ネットワークの例は、一般大衆（パーソナル・エリア・ネットワーク、又は、PANとして知られている）に接続されたネットワークや、自動車、列車、船、航空機のような乗り物に配置されたセンサのネットワークを含んでいる。飛行機、列車、バスなどのような大量輸送システムでは、管理者は、遠隔のホストに接続するためのラップトップ、パーソナル・デジタル・アシスタンス（PDA）、又は、自動車電話を使用可能とする常置の乗り物に搭載されたインターネット・アクセスを乗客に提供することも可能である。そのようなモバイル・ネットワーク内の個々のノードは、通常、中央の装置（すなわち、モバイル・ルータ）に接続され、ネットワークが動いている場合には接続点を変更せず、その代わり、ネットワーク全体が移動するように、モバイル・ルータが、その接続点を変更する。

【0005】

本発明は、移動中のネットワークの問題のために提案された解決策について記述するものである。本質的には、移動中のネットワークの問題は、全体として移動するネットワーク内のノードに対して、連続的なインターネット接続性を提供することである。移動するネットワーク内のノードは、ネットワークがインターネットへの接続点を変更していることに気付かないかもしれず、この点が、インターネット・プロトコル・バージョン4（IPv4）（非特許文献6）におけるモバイルIPv4（非特許文献5）や、インターネット・プロトコル・バージョン6（IPv6）（非特許文献8）におけるモバイルIPv6（非特許文献7）によって取り扱われているようなモビリティ・サポートの古典的問題とは異なっている。（非特許文献5、7）では、ネットワーク全体よりむしろ個々のホストに対して、モビリティ・サポートを提供することを主要な目的としている。

【0006】

モバイルIPでは、各モバイル・ノードは不変のホーム・ドメインを有している。モバイル・ノードが、そのホーム・ネットワークに接続されている場合、そのモバイル・ノードには、ホーム・アドレスとして知られる不変のグローバル・アドレスが割り当てられる。モバイル・ノードが離れている場合、すなわち、他のフォーリン・ネットワークに接続されている場合、モバイル・ノードには、気付アドレス (care-of-address) として知られる一時的なグローバル・アドレスが通常割り当てられる。モビリティ・サポートのアイデアは、たとえモバイル・ノードが他のフォーリン・ネットワークに接続された場合でも、モバイル・ノードがホーム・ドメインで到達可能となるようにするものである。これは、ホーム・エージェントとして知られるホーム・ネットワークのエンティティの導入によって、(非特許文献5、7)で行われている。モバイル・ノードは、バインディング・アップデートとして知られるメッセージを使用して、気付アドレスをホーム・エージェントに登録する。ホーム・エージェントは、モバイル・ノードのホーム・アドレスに出されたメッセージを傍受し、IP-in-IPトンネリング (非特許文献9、10) を使用して、モバイル・ノードの気付アドレスにパケットを転送しなければならない。IP-in-IPトンネリングは、オリジナルのIPパケットを別のパケットでカプセル化することを含んでいる。オリジナルのパケットは内部パケット (inner packet) と呼ばれることもあり、内部パケットをカプセル化する新しいパケットは外部パケット (outer packet) と呼ばれることもある。

【0007】

個々のホストのためのモビリティ・サポートの概念をノードのネットワークのためのモビリティ・サポートに拡張して、移動中のネットワークの解決策の目的は、インターネット上のどこにモバイル・ネットワークが接続しているかによらず、モバイル・ネットワーク内のノードが不変のアドレスによって到達可能となるメカニズムを提供することである。移動中のネットワークの問題を解決するための主要な試みがいくつか存在し、それらはすべて、モバイルIP (非特許文献5、7) に基づくものである。

【0008】

移動中のネットワークのために提案された解決策の1つは、モバイル・ルータ・サポート（非特許文献11）である。ここでは、モバイル・ネットワークを管理するモバイル・ルータがそのホーム・ドメインに存在する場合、モバイル・ルータが、いくつかのルーティング・プロトコルを使用してモバイル・ネットワークからの、又は、モバイル・ネットワークへのパケットのルーティングを行い、モバイル・ルータ及びそのモバイル・ネットワークがフォーリン・ドメインに移動する場合には、モバイル・ルータは、気付アドレスをそのホーム・エージェントに登録し、その後、IP-in-IPトンネルが、モバイル・ルータとホーム・エージェントとの間で設定される。モバイル・ルータがそのホーム・ドメインに存在する場合に使用されるルーティング・プロトコルは、IP-in-IPトンネル上でも再び実行される。これは、モバイル・ネットワークに向かうすべてのパケットが、ホーム・エージェントによって傍受され、IP-in-IPトンネルを通過してモバイル・ルータに転送されることを意味する。そして、モバイル・ルータは、そのモバイル・ネットワーク内のホストにパケットを転送する。そのモバイル・ネットワーク内のノードがネットワークの外にパケットを送りたい場合には、モバイル・ルータはパケットを傍受し、IP-in-IPトンネルを通過してホーム・エージェントにパケットを転送し、その後、ホーム・エージェントは意図された受信者にパケットを送信する。

【0009】

（非特許文献12）で提案された別の解決策は、モバイル・ルータ・サポート（非特許文献11）の拡張である。そこには、モバイル・ネットワークが入れ子になっている（すなわち、モバイル・ネットワークが別のモバイル・ネットワークに接続している）場合にあまりにも多くのレベルでカプセル化されることを回避するために、リバース・ルーティング・ヘッダを使用することが含まれている。ここでは、最低レベルのモバイル・ネットワークが、トンネル・パケットの中に、そのホーム・エージェントへのリバース・ルーティング・ヘッダを設定する。高いレベルのモバイル・ルータが途中でこのトンネル・パケットを傍受すると、より高いレベルのモバイル・ルータは、このパケットに関して、別のIP-in-IPトンネルへのカプセル化は行わず、代わりに、高いレベルのモバイル・ルータは

、リバース・ルーティング・ヘッダにパケット中のソース・アドレスをコピーし、ソース・アドレスとして、それ自身の気付アドレスを置く。このようにして、最初のモバイル・ルータのホーム・エージェントがパケットを受け取る場合、ホーム・エージェントは、最初のモバイル・ルータとホーム・エージェント自身との間のパスに存在するモバイル・ルータの連鎖を決定することができる。続いて、ホーム・エージェントが最初のモバイル・ルータに対して、別の傍受されたパケットを転送したい場合、パケットが他の高いレベルのモバイル・ルータに経由して最初のモバイル・ルータに直接送られるよう、転送されるパケットにルーティング・ヘッダ（非特許文献 8）を含ませることができる。

【0010】

移動中のネットワークの問題の 3 番目の解決策は、（非特許文献 13）で提案されており、プレフィックス・スコープ・バインディング・アップデートとして知られている。ここには、モバイル・ルータによって送られるバインディング・アップデートに、モバイル・ネットワークのプレフィックスに関する情報を付加する解決策が提案されている。このようにして、ホーム・エージェントは、バインディング・アップデートで特定されるものと等しいプレフィックスを持つノードはモバイル・ルータに接続されていると推定することができ、したがって、ホーム・エージェントは、これらのノードに向かうパケットを、そのモバイル・ルータに転送することができる。

【0011】

【発明が解決しようとする課題】

（非特許文献 11）では、IP-in-IP トンネルの使用は、ルート・トライアングュレーション（ルートの三角測量）として知られるものによって弊害が起こる。この弊害は、あるノードから別のノードまでのパケットが、出発地（ソース）と目的地（デスティネーション）との間の最短経路上に位置していない第三者（この場合、ホーム・エージェント）を通り抜ける必要がある場合に生じ、モバイル・ネットワークが入れ子となっている場合に、ルート・トライアングュレーションの影響が含まれる。例えば、3 つのモバイル・ルータを通して転送される必要のあるモバイル・ネットワークからのパケットを考慮する。（非特許文献 11）

で提案される解決策を使用して、パケットは3つの異なるトンネルの中でカプセル化されなければならない。ここで、各トンネルは、異なるモバイル・ルータの異なるホーム・エージェントに向かうものである。この多数のトンネリングは、パケットの配達に相当な遅れをもたらすだけではなく、カプセル化によって全体のパケット・サイズが増加するので、途中でパケットがフラグメント化される可能性を増大させる。フラグメント化されたパケットの再集合は、さらなる処理の遅れを導き、フラグメントのうちの1つが途中で失われた場合、パケット全体が破棄されることにもなる。

【0012】

(非特許文献12)で提案された解決策は、多数のトンネルを回避することによって、この問題の解決を試みている。この解決策では、最初のモバイル・ルータが、そのホーム・エージェントとのIP-in-IPトンネルを設定すればよい。その後のモバイル・ルータは、さらにパケットをカプセル化することではなく、代わりに、これらのルータは、オリジナルのソース・アドレスにリバース・ルーティング・ヘッダを記録し、ソース・アドレスを気付アドレスに変更し、それらのホーム・エージェントを通り抜けずに、その目的地にパケットを転送する。この解決策は非常に効率的なやり方で多数のトンネルの問題を解決するが、リバース・ルーティング・ヘッダに記録されたアドレスのリストが信頼すべきものであることをホーム・エージェントが確認することは非常に困難である。(非特許文献12)では、どのようなパケットでも直接モバイル・ルータに転送するルーティング・ヘッダを構築するため、リバース・ルーティング・ヘッダ内においてアドレスのリストを利用するホーム・エージェントが要求されるので、ホーム・エージェントが、リバース・ルーティング・ヘッダに記録されたアドレスが正当なものであると確証できることは重大である。(非特許文献12)の解決策は、リバース・ルーティング・ヘッダがさらされる安全性への脅威に対して、何の改善法も供給しない。

【0013】

多数のトンネリングの問題を解決するための別の単純な解決策は、後段のモバイル・ルータが外部パケットを指定された目的地に直接転送できるようにするこ

とである（さらに、後段のモバイル・ルータのホーム・エージェントへのトンネリングのレベルで外部パケットのカプセル化を行う代わりに）。しかしながら、それでも、最も外側のパケットが正当なソースから来たことを受信者は確認できないので、同じセキュリティの問題に直面する。

【0014】

【課題を解決するための手段】

セクション3.3に挙げられた問題を解決するため、本発明は、モバイル・ネットワーク・エレメントが、モバイル・ノードが接続されているアクセス・ルータに関する情報をそのホーム・エージェント又は他の対応ノード (corresponding node) に渡すためのメカニズムを使用する。この情報を使用して、ホーム・エージェント又は対応ノードは、ルート・トライアングレーションで加わるペナルティを招かずに、モバイル・ノードにパケットを直接送るためのルーティング・ヘッダを構築することが可能となる。モバイル・ノードが接続されているルータに関する情報はモバイル・ノード自身によって送られるので、情報の確実性は必然的に確立される。

【0015】

さらに、ホーム・エージェント又は他の対応ノードは、モバイル・ノードが接続されているルータに関する情報を受信したので、アクセス・ルータのうちの1つである外部のソース・アドレスを備えてトンネルから到着するパケットが、正当なソースから来たことを確認することができる。したがって、受信者が転送するルータの信頼性を確認できるので、モバイル・ルータは、外部パケットを直接指定された目的地に転送することが可能である。

【0016】

【発明の作用】

本発明は、パケット交換データ・ネットワークのインターネットワーキングを含んでいる。これらのネットワークのうちのいくつかは移動しており、例えば、前記ネットワークの内部ネットワーク側インターフェイスを制御するルータは、その接続点を変更するものである。本発明は、ローミングするホストへのグローバルな接続性を提供するために既存の解決策の拡張を提供し、その結果、ローミ

ングするホストへのグローバルな接続性も達成可能となる。

【0017】

本発明は、3つの主要なタイプのノードで使用されるいくつかのアルゴリズムが開示した。これらは、グローバルなデータ通信網への接続点を変更するモバイル・ホスト、移動するネットワークの内部ネットワーク側インターフェイスを制御するモバイル・ルータ、モバイル・ホスト及びモバイル・ルータと通信を行うグローバルなデータ通信網上の他のホストである。これらのアルゴリズムを十分に展開して、移動するネットワークへのパケット、又は、移動するネットワークからのパケットを最小の遅延で、意図された目的地に配信することが可能である。

【0018】

【発明の実施の形態】

このセクションでは、ローミング・ネットワークへのグローバルな接続を提供するための方法が開示される。開示される発明の理解を支援するため、次の定義が使用される

【0019】

・「パケット」はデータ・ネットワーク上で伝送可能とするあらゆるフォーマットが可能なデータの自己独立型ユニットである。「パケット」は、通常、「ヘッダ」及び「ペイロード」部分の2つの部分によって構成される。「ペイロード」部分は、伝送されるデータを含んでおり、「ヘッダ」部分は、パケットの伝送を援助するための情報を含んでいる。「ヘッダ」は、「パケット」の送信者と受信者とをそれぞれ識別するためのソース・アドレス及び終点アドレスを持たなければならない。

【0020】

・「パケット・トンネリング」は、別のパケットにカプセル化されている自己独立型パケットである。「パケット・トンネリング」の動作は、パケットの「カプセル化」とも呼ばれる。また、カプセルに入れられているパケットは「トンネル化されたパケット」又は「内部パケット」と呼ばれ、「内部パケット」をカプセルに入れるパケットは「トンネリング・パケット」又は「外部パケット」と呼ば

れる。ここで、「内部パケット」全体は、「外部パケット」のペイロード部分を形成している。

【0021】

・「モバイル・ノード」は、グローバルなデータ通信網との接続点を変更するネットワーク・エレメントであり、それは、エンド・ユーザ端末、又は、グローバルなデータ通信網との接続点を変更することができるゲートウェイ、ルータ、インテリジェント・ネットワーク・ハブとして機能する中間ネットワーク・エレメントに関連して使用されてもよい。エンド・ユーザ端末である「モバイル・ノード」は、より明確に「モバイル・ホスト」と呼ばれる一方、ゲートウェイ、ルータ、又は、インテリジェント・ネットワーク・ハブとして機能する中間ネットワーク・エレメントである「モバイル・ノード」は、より明確に「モバイル・ルータ」と呼ばれる。

【0022】

・モバイル・ノードの「アクセス・ルータ」は、ゲートウェイ、ルータ、又は、インテリジェント・ネットワーク・ハブとして機能する中間ネットワーク・エレメントであり、前述のモバイル・ノードが、前述のネットワーク・エレメントを通じてグローバルなデータ通信網へのアクセスを獲得するために接続するものである。

【0023】

・「ホーム・アドレス」は、モバイル・ノードに割り当てられた主要なグローバル・アドレスであり、現在モバイル・ノードがグローバルなデータ通信網上のどこに接続しているかによらず、モバイル・ノードに到達可能とするために使用されるものである。

【0024】

・そのホーム・アドレスが接続点の近くで使用されるアドレスとトポロジカルに互換性を持つグローバルなデータ通信網に接続されるモバイル・ノードは、「ホームにいる (at home)」と呼ばれ、単一の管理ドメインによってコントロールされるこの接続点の近傍は、モバイル・ノードの「ホーム・ドメイン」と呼ばれる。

【0025】

・そのホーム・アドレスが接続点の近くで使用されるアドレスとトポロジカルに非互換性を持つグローバルなデータ通信網に接続されるモバイル・ノードは、「離れている (away)」と呼ばれ、単一の管理ドメインによってコントロールされるこの接続点の近傍は、モバイル・ノードの「フォーリン・ドメイン」と呼ばれる。

【0026】

・「気付アドレス (care-of-address)」は、離れているモバイル・ノードに割り当てられる一時的なグローバル・アドレスであり、割り当てられた「気付アドレス」は、グローバルなデータ通信網への接続点の近傍で使用されるアドレスとトポロジカルに互換性を持つものである。一般に、「気付アドレス」は、モバイル・ノードが同一のアクセス・ルータに接続されているだけ有効である。

【0027】

・「ホーム・エージェント」は、モバイル・ノードのホーム・ドメインに存在するネットワーク・エンティティであり、モバイル・ノードが離れている場合に、モバイル・ノードの気付アドレスの登録サービスを行って、モバイル・ノードのホーム・アドレスに宛てられたパケットを、モバイル・ノードの気付アドレスに転送するものである。

【0028】

・「対応ノード (corresponding node)」は、モバイル・ノードが通信を行っているグローバルなデータ通信網上にあるすべてのネットワーク・エレメントに対応するものである。

【0029】

・「バインディング・アップデート (binding update)」は、モバイル・ノードからそのホーム・エージェント又は対応ノードに対して送られるメッセージであり、送信者 (モバイル・ノード) の現在の気付アドレスを受信者 (ホーム・エージェント又は対応ノード) に通知するものである。これによって、受信者側において、モバイル・ノードの気付アドレスとホーム・アドレスとの間に「バインディング (binding)」が作られる。

【0030】

・「バインディング・アックノレジメント (binding acknowledgement)」は、バインディング・アップデートのメッセージの受信者から前述のバインディング・アップデートのメッセージの送信者に対して送られるメッセージであり、バインディングの結果を示すものである。

【0031】

・「ルーティング・ヘッダ」は、パケットに付加される1つの情報であり、パケットが転送されるべきグローバルなデータ通信網内の中間ルータを指示する情報である。通常、グローバルなデータ通信網内のルータは、目的地に基づいてパケットを転送するが、「ルーティング・ヘッダ」は、中間の目的地のリストを含むことにより、その振る舞いを上書きする。「ルーティング・ヘッダ」を使用するため、送信者は、ルーティング・ヘッダの最後のエントリに、意図された受信者のアドレスを入れ、パケットの終点アドレスに、最初の中間の目的地 (first intermediate destination) を置く。最初の目的地は、パケットを受け取って「ルーティング・ヘッダ」を備えたパケットを更新し、その後、パケットが2番目の中間の目的地に転送されるようにする（すなわち、パケットの終点アドレスは、「ルーティング・ヘッダ」内の次のエントリと交換される）。そのサイクルは、最後の中間の目的地に到達するまで繰り返され、「ルーティング・ヘッダ」は更新されて、その結果、パケットが実際の意図された目的地に転送される。「ルーティング・ヘッダ」のオペレーションのより詳細な説明を求める場合には、読者は[非特許文献8]を参照すべきである。

【0032】

・本発明で開示された方法及びメカニズムを支援又は実施するあらゆるネットワーク・エレメントは、「発明を可能とする」ネットワーク・エレメントと呼ばれる。

【0033】

以下の記述では、説明のため、具体的な数、時間、構造、その他のパラメータが、本発明を完全に理解するために示されるが、このような具体的な詳細がなくとも、本発明を実施できることは当業者にとっては明白だろう。

【0034】

開示される発明が、本発明で開示される方法及びメカニズムを支援しないネットワーク・エレメントを含むグローバルなデータ通信網において共存するため、発明を可能とする何らかのルータが、このドキュメントに示された方法及びメカニズムを使用することができることをそれらに示さなくてはならない。これは、ルータが、隣接装置に対して時々ブロードキャストするメッセージの中に、ユニークな信号を挿入することによって達成されるであろう。ネットワーク・エレメントが他のネットワーク・ノードにそれらの能力を通知することができる様々な既存の方法を、当業者なら認識できるはずである。さらに、前述のモバイル・ルータからの特定のブロードキャスト・メッセージによって、モバイル・ルータによって制御されるネットワーク・セグメントに接続するモバイル・ノードが、前述のモバイル・ルータのホーム・アドレスを知ることが可能なはずである。

【0035】

例えば、インターネット・プロトコル・バージョン6[非特許文献8]の状況では、ホーム・アドレス・オプションを、そのホーム・アドレスを広告するための発明を可能とするルータによって、送られるIPv6近隣探索[非特許文献14]で特定されるルータ・アドバタイズメント・メッセージに挿入することが可能である。ホーム・アドレス・オプションは、次のフィールドを含むべきである：請求項3に記載されるような(1)このオプションをホーム・アドレス・オプションと識別できるタイプ・フィールド、(2)このオプションのサイズを示すレンジ・フィールド、及び、(3)送信者のホーム・アドレスを特定するホーム・アドレス・フィールド。

【0036】

発明を可能とするルータによって送られたブロードキャスト・メッセージから、その後、モバイル・ノードは、請求項1に記載されるように、モバイル・ノードによって送られるバインディング・アップデートにおいて、モバイル・ノードが接続されるアクセス・ルータのホーム・アドレスを有することができるようになる。アクセス・ルータが発明を可能とするものである場合に限り、これは可能である。様々な可能な異なる方法で、そのような情報をバインディング・アップ

データ・メッセージに埋め込むことが可能であり、グローバルなデータ通信網で使用される基本のプロトコルに依存している。例えば、インターネット・プロトコル・バージョン 6（非特許文献 8）の状況では、アクセス・ルータ・アドレス・オプションは、モバイル IP v 6（非特許文献 7）に規定されるバインディング・アップデート・メッセージに挿入可能であり、そのようなオプションは、次のフィールドを含むべきである：請求項 2 に記載されるような（1）このオプションをアクセス・ルータ・ホーム・アドレスと識別できるアクセス・ルータ・アドレス・オプション、（2）このオプションのサイズを示すレングス・フィールド、及び、（3）送信者が接続されているアクセス・ルータのホーム・アドレスを特定するアクセス・ルータ・アドレス・フィールド。

【0037】

発明が可能となる受信者（モバイル・ノード又は対応ノードのホーム・エージェントかもしれない）が、このバインディング・アップデートを受け取った場合、受信者は、これをテーブル又はリストに記録することが可能である。以降バインディング・エントリと呼ぶことにするこのようなテーブル又はリスト中のエントリは、少なくとも、次の 3 つのフィールドを含むべきである：請求項 5 に記載されるような（1）モバイル・ノードのホーム・アドレスを含むホーム・アドレス・フィールド、（2）モバイル・ノードの気付アドレスを含む気付アドレス、及び、（3）アクセス・ルータのホーム・アドレスを含むアクセス・ルータ・アドレス・フィールド。これらの 3 つのフィールドの値は、バインディング・アップデート・メッセージから抽出することが可能である。

【0038】

図 1 は、請求項 6 に記載されるように、発明を可能とするネットワーク・エレメントがバインディング・アップデート・メッセージを受け取る場合に、バインディング・エントリを更新するために使用されるアルゴリズムを図示するものである。符号 101 で記されるステップにおいて、バインディング・エントリ内で、バインディング・アップデート・メッセージ内のホーム・アドレスと同等のホーム・アドレス・フィールドのエントリが検索される。もし見つからない場合には、符号 102 及び 103 で記されるステップに示されるように、新たなエント

りが作られる。また、バインディング・アップデート・メッセージに気付アドレスが含まれていない場合、又は、気付アドレスがホーム・アドレスと同じものである場合、バインディング・アップデートの送信者は、そのホーム・ドメインに戻っており、したがって、符号104、105及び106で記されるステップで示されるように、バインディング・エントリからそのエントリが削除されたと仮定される。一方、バインディング・アップデート・メッセージに気付アドレスが含まれている場合には、エントリ内の気付アドレス・フィールドは、符号107で記されるステップで示されるように、バインディング・アップデート・メッセージ内で特定される気付アドレスに更新される。また、バインディング・アップデート・メッセージがアクセス・ルータのホーム・アドレスを含んでいる場合には、符号108及び109で記されるステップで示されるように、エントリ内のアクセス・ルータ・アドレス・フィールドが更新される。一方、バインディング・アップデート・メッセージがアクセス・ルータのホーム・アドレスを含んでいる場合には、バインディング・アップデートの送信者は、現在、発明を可能としないアクセス・ルータに接続されていると仮定され、この場合、符号110で記されるステップで示されるように、アクセス・ルータ・アドレス・フィールドには無効である旨が記される。

【0039】

バインディング・アップデートの送信者は、自由にバインディング・アクノレヅジメントを要求することができ、これによって、バインディング・アップデートの受信者は送信者に対して、アップデートの結果を通知することが可能となる。有効なアクセス・ルータ・アドレス情報を含んでいるバインディング・アップデート受信する発明を可能とする受信者が、バインディング・アクノレヅジメントで返答を行う場合、請求項4に関連して、バインディング・アクノレヅジメントの送信者が発明を可能とするものである旨をバインディング・アクノレヅジメントの受信者が推測できるような方法で、バインディング・アクノレヅジメントに指標が定められなければならない。そのような指標は、例えば、ビット・フラグやバインディング・アクノレヅジメントのビット・ストリームの特定のパターンやこれらに限定されない様々な方法で達成されることは、当業者にとって明白

である。

【0040】

バインディング・エントリを使用して、対応ノード又はホーム・エージェントは、モバイル・ノードに直接到達可能なルーティング・ヘッダを構築することが可能である。ルーティング・ヘッダは、まず、パケットがアクセス・ルータのホーム・アドレスに転送され、その後、モバイル・ノードの気付アドレスに転送されるよう、構築することが可能である。このように、パケットは、モバイル・ノードのホーム・ドメインを横断する必要がなく、ホーム・エージェントによって傍受され、その後、気付アドレスでモバイル・ノードに転送される。

【0041】

もし、アクセス・ルータ自身が移動可能で離れている (away) 場合には、たとえば、ルーティング・ヘッダが使用されても、依然としてパケットは遠回りのルートをたどることとなる。これは、アクセス・ルータが離れているので、アクセス・ルータのホーム・アドレスに転送されるパケットがアクセス・ルータのホーム・ドメインにルートが定められるせいである。アクセス・ルータのホーム・エージェントはパケットを遮り、アクセス・ルータの気付アドレスでアクセス・ルータにパケットを転送する。

【0042】

発明を可能とするアクセス・ルータが、発明を可能とするホーム・エージェント及びモバイル・ノードの対応ノードに対してバインディング・アップデートを送るようにすることにより、さらにパケットの配送を最適化することが可能となるかもしれない。また、アクセス・ルータが発明を可能とするものであるならば、アクセス・ルータ自身のホーム・アドレスをバインディング・アップデート内に付加すべきである。アクセス・ルータが移動する場合 (移動可能な場合) に著しい遅延を招かないようにするため、いかなる発明を可能とするモバイル・ノードも、バインディング・アップデートを送った他のホスト (ホーム・エージェント及び対応ノードの両方) のリストを維持すべきである。以降、このリストをバウンド・ホスト・リスト (Bound Hosts List) と呼ぶことにする。モバイル・ノードが移動する場合には、モバイル・ノードは、それぞれのホストにバインデ

イング・アップデートを送ることによって、バウンド・ホスト・リスト上のホストに通知すべきであるが、モバイル・ノードが移動するたびにバインディング・アップデートの突発を導いてしまうことを避けるため、バインディング・アップデートの連続的な送信間で少しずらすべきである。

【0043】

発明を可能とするモバイル・ノード及びアクセス・ルータが、バインディング・アップデートでホストに通知を行う場合、いかなる発明を可能とするホーム・エージェント又は対応ノードも、モバイル・ノードへのパケットの配送を最適化するためのモバイル・ノード周辺のネットワーク・トポロジに関する知識を十分に獲得することができる。そうするためには、請求項7に記載されているように、バインディング・エントリからのルーティング・ヘッダを構築する場合に、図2に描かれたアルゴリズムを使用することが可能である。

【0044】

このアルゴリズムでは、スタック（ラスト・イン・ファースト・アウト情報蓄積構造）がルーティング・ヘッダの構築を援助するために使用される。符号201で記されるステップにおいて、スタックは空となるよう初期化され、さらに、符号202で記されるステップで示されるように、2つの一時的変数src及びdstが、パケットのソースの（すなわち、パケットを送るホーム・エージェント又は対応ノード）アドレス及び終点アドレス（すなわち、モバイル・ノードのホーム・アドレス）のそれぞれに設定される。その後、アルゴリズムは、符号203～209で記されるステップのループに入り、そのループでは、dstに格納された値と等しいホーム・アドレス・フィールドを備えたエントリを求めて、バインディング・エントリが検索される。何も見つからない場合には、符号203及び204で記されるステップで示されるようにループを出て、一方、エントリが見つかる場合には、dstの中の値がチェックされて、その値がモバイル・ノードのホーム・アドレスかどうかを確認される（ループの1回目の繰り返しの1度目だけで正しい結果が出るべきである）。その値がモバイル・ノードのホーム・アドレスであることが確認された場合、符号204、205及び206で記されるステップで示されるように、dstの中の値がスタックに入れられる。

【0045】

次に、アルゴリズムは、符号207で記されるステップで示されるように、バインディング・エントリ内で発見された気付アドレス・フィールドに格納するdstの中の値を更新する。その後、バインディング・エントリのアクセス・ルータ・アドレス・フィールドはチェックされ、有効なアドレスを含んでいるかどうかを確認される。有効なアドレスを含んでいる場合には、符号208及び209で記されるステップで示されるように、ループが繰り返される。ステップ209において、dstフィールドの内容もスタックに入れられ、アクセス・ルータ・フィールドが無効である場合には、ループが出る。いったんループから出た場合、符号210及び211で記されるステップで示されるように、スタック内の内容は、逆の順に押し出されて、ルーティング・ヘッダに追加される。また、スタックが空になった場合には、ステップ212で記されるステップに示されるように、パケットの終点フィールドはdstに格納された値に設定され、アルゴリズムは終了となる。

【0046】

一方、このように構築されたルーティング・ヘッダは、モバイル・ノードに配送されるパケットのルーティングを最適化することが可能であるが、それは、あるセキュリティの脅威を導くことにもなる。最も顕著な脅威は、攻撃者が、モバイル・ネットワーク中のノードからパケットが反射されるような特定のルーティング・ヘッダを構築することができ、その結果、攻撃者は、他の方法ではアクセス不可能なグローバルなデータ通信網の部分に到達することが可能となる。そのようなセキュリティ違反を回避するため、いかなる発明を可能とするモバイル・ノードも、偽りであると疑問に思われるすべてのパケットを破棄するための図3及び4の中で描かれたアルゴリズムを従うべきである。

【0047】

図3で図示されたアルゴリズムは、発明を可能とするルータによって使用されるものである。パケットがルータによって傍受されると、符号301及び303で記されるステップで示されるように、まず、ルータは終点アドレスがそのホーム・アドレス又はその気付アドレスと等しいかどうかをチェックする。もし終点

アドレスがホーム・アドレスと等しい場合には、符号 302 で記されるステップで示されるように、パケットが消費される。また、もし終点アドレスが気付アドレスと等しい場合には、符号 304 で記されるステップで示されるように、ルーティング・ヘッダの存在がチェックされる。また、もし終点アドレスがホーム・アドレスでも気付アドレスでもない場合には、符号 305 で記されるステップで示されるように、終点アドレスが、ルータに接続されたローカル・ネットワーク内の有効なアドレスであるかどうかチェックされる。終点アドレスがルータに接続されたローカル・ネットワーク内の有効なアドレスである場合、符号 311 で記されるステップで示されるように、パケットはその目的地に転送され、そうでなければ、符号 310 で記されるステップで示されるように、パケットは破棄される。

【0048】

また、符号 304 で記されるステップにおいて、ルーティング・ヘッダの存在がチェックされ、存在しない場合には、符号 310 で記されるステップで示されるように、パケットが破棄される。また、ルーティング・ヘッダが存在すれば、ルーティング・ヘッダ内の次のアドレスが最後のエントリであるかどうかチェックされる。ルーティング・ヘッダ内の次のアドレスが最後のエントリではない場合、エントリはパケットの終点アドレスと入れ換えられて、符号 306、307、305 に記されるステップで示されるように、終点アドレスが、ルータに接続されたローカル・ネットワーク内の有効なアドレスであるかどうか再チェックされる、ルータ・ヘッダ内の次のアドレスが最後のエントリである場合、符号 306 及び 308 で記されるステップで示されるように、この最後のエントリはチェックされて、それがルータのホーム・アドレスであるかどうか確認される。それがホーム・アドレスである場合には、符号 309 で記されるステップで示されるように、パケットが消費され、そうでない場合には、符号 310 で記されるステップで示されるように、パケットは破棄される。

【0049】

図 4 に示されるアルゴリズムは、モバイル・ホスト（すなわち、ルータとして機能していないモバイル・ノード）が使用するものである。まず、符号 401 で

記されるステップにおいて、終点アドレスはチェックされて、モバイル・ノードのホーム・アドレスかどうかを確認される。もしYesならば、符号406で記されるステップで示されるように、パケットは消費され、そうでないならば、符号402で記されるステップで示されるように、終点アドレスはチェックされ、モバイル・ノードの気付アドレスかどうかを確認される。終点アドレスがモバイル・ノードの気付アドレスではない場合には、符号407で記されるステップで示されるように、パケットが破棄され、一方、終点アドレスがモバイル・ノードの気付アドレスと等しい場合には、ルーティング・ヘッダの存在がチェックされる。さらに、符号403、404及び405で記される一連の確認ステップで示されるように、ルーティング・ヘッダのエントリの残りはあと1つであり、そのエントリはモバイル・ノードのホーム・アドレスのはずである。符号407で記されるステップで示されるように、これらのテストのうちのどれかが失敗した場合には、パケットが破棄され、すべてのテストを通過した場合には、符号406で記されるステップで示されるように、パケットが消費される。

【0050】

上記では、モバイル・ノード及びアクセス・ルータのホーム・エージェントを通ることなく、モバイル・ノードにパケットを配送する方法を十分に説明、それによって、配送遅延 (delivery latency) を減少させている。次に開示される部分では、モバイル・ノードから送られるパケットに注目する。ここで注意すべき点は、離れているモバイル・ノードがパケットを送る場合、パケット・ソースとしてその気付アドレスを使用することである。配置された多くのパケット交換ネットワークでは、イングレス・フィルタリング (ingress filtering) がセキュリティを理由として使用されるので、これが行われる。イングレス・フィルタリングは、破棄されたパケットがローカル・ネットワーク内で使用されるアドレスとトポロジカルに非互換性のソース・アドレスを持つので、前述のローカル・ネットワークから出るパケットの破棄を適用するものである。離れているモバイル・ノードがフォーリン・ドメインの内部からパケットを送るために、ソース・アドレスとしてそのホーム・アドレスを使用する場合には、パケットはイングレス・フィルタリングによって破棄される可能性がある。したがって、イングレス・

フィルタリングを回避するために、気付アドレス（フォーリン・ドメイン内で使用されるアドレスとトポロジカルに互換性を持つアドレス）が、ソース・アドレスとして使用される。受信者がパケットの作成者を識別するのを助けるために、離れているモバイル・ノードは、パケットのヘッダにそのホーム・アドレスを含ませる。したがって、まとめると、離れているモバイル・ノードがパケットを送る場合は常に、パケットのソース・アドレスに気付アドレスを記し、特別な情報としてパケット・ヘッダにそのホーム・アドレスを挿入する。

【0051】

そのアクセス・ルータが発明を可能とするものであることをモバイル・ノードが気づいている場合、それによって、アクセス・ルータとアクセス・ルータのホーム・エージェントとの間でパケットがトンネリングすることなく、モバイル・ノードが送ったパケットをアクセス・ルータが直接目的地に転送することが可能となる。請求項8に関連して、これは、パケット・ヘッダに信号を挿入することによって実行可能となる。この信号は、ビット又は特別のパターンのビット・ストリームのような任意の形式とすることが可能である。このような信号の存在によって、いかなるパケット・トンネリング又はカプセル化技術も使用せずに、パケットの送信者が目的地にパケットを直接転送する試みをルータに要求していることが、発明を可能とするルータに示される。このドキュメントでは、以降、この信号は「直接転送要求 (direct-forwarding-request)」と呼ぶことにする。また、請求項9に関連して、後段のルータがパケット・トンネリング又はカプセル化技術を使用せずに目的地にパケットを直接転送する試みを望まない場合、中間ルータは、直接転送要求信号を無効にすることも可能である。発明を可能とするモバイル・ルータがこのパケットを傍受し、特別にパケットに直接転送要求が記載されていることに気づいた場合には、モバイル・ルータは、パケットのソース・アドレスがそのローカル・ネットワークからの有効なアドレスかどうかをチェックする。もし行われなない場合には、このパケットの作成者とルータ自身の間に少なくとも1つの発明を可能としない中間ネットワーク・エレメントが存在することを意味し、この場合、ルータは直接の転送を実行することができない。次に、モバイル・ルータは、パケットが特定の目的地を備えたバインディング・ア

アップデートを持っているかどうかをチェックする。そうであれば、モバイル・ルータは、ソース・アドレスを気付アドレスに変更し、目的地にパケットを送る。一方、他の場合に関しては、パケットはカプセル化されてモバイル・ルータのホーム・エージェントにトンネリングされ、モバイル・ルータのホーム・エージェントで脱カプセル化 (decapsulated) されて、実際の目的地に配送される。もちろん、これはモバイル・ルータがホームから離れていることが前提となっており、ホームに存在する場合には、直接転送要求をチェックする必要はない。モバイル・ルータが傍受するそのローカル・ネットワークからのすべてのパケットは、ホーム・エージェントにパケットをトンネリングする必要はなく、デフォルトによって目的地に転送される。

【0052】

請求項10に関連して、これは図5に示されるブロックダイアグラムで図示される。ホームから離れている発明を可能とするモバイル・ルータがパケットを傍受する場合、符号501で記されるステップで示されるように、まず、モバイル・ルータは、パケットが直接転送要求で特徴づけられるかどうかをチェックする。次に、符号502で記されるステップで示されるように、パケット内のソース・アドレスが、モバイル・ルータのローカル・ネットワーク内の有効なアドレスであること確認される。そして、最後に、符号503で記されるステップで示されるように、指定された目的地がチェックされ、モバイル・ルータが以前バインディング・アップデートを送ったところかどうかを確認される。3つのテストのうちのどれかが否定の答えである場合、符号504で記されるステップで示されるように、パケットは、トンネリングを使用してホーム・エージェントに転送される。一方、そうでなければ、符号505で記されるステップで示されるように、パケットは直接転送される。ここで、発明を可能とするモバイル・ルータはパケット・ヘッダを修正し、その結果、ソース・アドレスが気付アドレスによって置き換えられることとなる。

【0053】

パケットのソース・アドレスがルータによって途中で変更されるので、パケットが信頼あるソースから送出されたことをパケットの受信者が確認するための方

法が存在しなくてはならない。パケット・ヘッダ内にパケットを送るモバイル・ノードのホーム・アドレスを包含することは、確認方法の形式の1つを提供する。しかしながら、攻撃者はパケットを偽造し、パケット・ヘッダにホーム・アドレス情報を偽って挿入することが可能である。したがって、受け取ったパケット内のソース・アドレスが、許可を受けた発明を可能とする送信者（この送信者は、指定されたホーム・アドレスを備えたモバイル・ノードに関するものである）のアクセス・ルータであると受信者が確認できることが非常に重要である。そのための方法の1つとして、バインディング・エントリを介してチェックする方法が存在し、これによって、受信パケットのソース・アドレスがパケット・ヘッダに挿入されたホーム・アドレスにリンクされていることが確認される。また、請求項11に関して、図6は、そのような関係を確認するアルゴリズムを示すものである。

【0054】

図6の中で示されるアルゴリズムは、関係が確認可能な場合にブール値TRUEを返し、そうでなければブール値FALSEを返す。まずアルゴリズムが開始されると、符号601で記されるステップで示されるように、パケット・ヘッダ内で特定されるホーム・アドレスを格納するために、変数tempが最初に初期化される。その後、アルゴリズムは、バインディング・エントリを詳細に調べるためにループ（符号602～607で記されるループ）に入る。最初に、tempの中の値がパケットのソース・アドレスと確認し合わされる。それらが等しい場合には、符号602で記されるステップで示されるように、アルゴリズムはTRUEを返し、それらが等しくない場合には、符号603で記されるステップで示されるように、tempに格納された値と等しいホーム・アドレス・フィールドを備えたバインディング・エントリ内のエントリが探索される。何も見つからない場合には、符号604で記されるステップで示されるように、アルゴリズムはFALSEを返し、もし、そのようなエントリが見つかる場合には、符号605で記されるステップで示されるように、パケットのソース・アドレスが、発見されたエントリの気付アドレス・フィールドと比較される。その2つが同一の場合、関係は確認されてアルゴリズムはTRUEを返し、同一でない場合には、符号606で記されるステップで示さ

れるように、発見されたエントリのアクセス・ルータ・アドレス・フィールドが有効なエントリを含んでいるかどうかチェックされる。アクセス・ルータ・アドレス・フィールドが無効の場合には、アルゴリズムはFALSEを返し、アクセス・ルータ・アドレス・フィールドが有効の場合には、アクセス・ルータ・アドレス・フィールド内のアドレスがtempに格納され、符号607で記されるステップで示されるように、ループが反復される。

【0055】

請求項18に関連して、発明を可能とする基本的なノードは、バインディング・エントリ、及び、図1に示され請求項6に記載されるようなバインディング・エントリを更新するアルゴリズムを実行する必要がある。さらに、請求項4に記載されるように、それは、対応するバインディング・アップデート・メッセージ内のアクセス・ルータのホーム・アドレスに関する情報が受理されることをバインディング・アクノレジメントの受信者が認識できるようにする特別の情報で、バインディング・アクノレジメントを特徴付けるべきである。さらに、セキュリティ関係については、発明を可能とするノードが、図6に示され請求項11に記載されるような受信パケットのソース・アドレスをチェックするアルゴリズムを実施する必要がある。結局、発明を可能とするモバイル・ノードに対するパケットの配送を最適化することができるよう、発明を可能とする基本的なノードは、図2に示され請求項7に記載されるようなルーティング・ヘッダを構築するためのアルゴリズムを実施する必要がある。

【0056】

また、請求項12及び13に関連して、発明を可能とするノードは、バインディング・アップデート・メッセージの送信者が接続されているアクセス・ルータのホーム・アドレスに関する付属情報を持つバインディング・アップデート・メッセージの受理から短い時間の後に、特定のアクセス・ルータを通じて前述の送信者に対してパケットの転送を開始することとなる。これは、バインディング・アップデートの受理の後に、発明を可能とするノードから送信される任意のパケットが、次の特徴のうちの1つを持っていることを意味する：(1) 前述のパケットは、アクセス・ルータのホーム・アドレスに設定されるソース・アドレス

・フィールドを有しており、バインディング・アップデートの前述の送信者の気付アドレス及びホーム・アドレスだけを含んでいるルーティング・ヘッダが添えられているか、又は、(2) 前述のパケットは、アクセス・ルータのホーム・アドレスに設定されるソース・アドレス・フィールドを有しており、最初のエントリとしてバインディング・アップデートの前述の送信者の気付アドレスを含んでいるルーティング・ヘッダが添えられている。

【0057】

前述のアクセス・ルータは、バインディング・アップデートに同じ発明を可能とする同一ノードに対して、その気付アドレスを含むバインディング・アップデートも送信すべきであり、発明を可能とするノードから送られるパケットは、次の特徴のうちの1つを持っている：(1) 前述のパケットは、アクセス・ルータの気付アドレスに設定されるソース・アドレス・フィールドを有しており、バインディング・アップデートの前述の送信者の気付アドレス及びホーム・アドレスだけを含んでいるルーティング・ヘッダが添えられているか、(2) 前述のパケットは、アクセス・ルータの気付アドレスに設定されるソース・アドレス・フィールドを有しており、最初のエントリとしてバインディング・アップデートの前述の送信者の気付アドレスを含んでいるルーティング・ヘッダが添えられているか、又は、(3) 前述のパケットは、バインディング・アップデート及びアクセス・ルータの前述の送信者及びアクセス・ルータの気付アドレスを含んでいるルーティング・ヘッダが添えられており、そこでは、請求項14、15及び16に記載されるように、アクセス・ルータの気付アドレスがバインディング・アップデートの前述の送信者の気付アドレスの直前に来る。

【0058】

発明を可能とするモバイル・ノードには、請求項19に関連して、発明を可能とする基本的なノードのために記述されたそれらの機能に加えて、請求項8に記載されるようなパケット内に直接転送要求を挿入する機能と、請求項1に記載されるようなバインディング・アップデート・メッセージ内にそのアクセス・ルータのホーム・アドレスを挿入するための機能とが実施されなければならない。もし、モバイル・ノードがモバイル・ルータとして機能しない場合には、図4で図

示されるような入力パケットをチェックするアルゴリズムも実施されなければならない。

【0059】

請求項20に関連して、発明を可能とするモバイル・ルータは、発明を可能とするモバイル・ノードに明記されたものに加えて、図5に記述されて請求項10に記載されるように、直接転送要求信号を求めてローカル・ネットワーク（すなわち、前述のルータの内部ネットワーク側インターフェイス（ingress interface））からのパケットをチェックする機能を実行しなければならない。さらに、ルータは、図3に示されるような外部ネットワーク側インターフェイス（egress interface）から到着するパケットに関して、セキュリティ・チェックを実行しなければならない。

【0060】

また、請求項17に関連して、発明を可能とするノードは、その内部ネットワーク側インターフェイスから直接転送要求信号を含むパケットを受け取った後に、単に、前述のパケットのソース・アドレスを、単にそれ自身の気付アドレス又はホーム・アドレスに変更することによって、パケットを転送することが可能である。これは、アクセス・ルータのバウンド・ホスト・リストがパケットの目的地フィールドに明記されたホストを含む場合に起こり、もし、明記された目的地がバウンド・ホスト・リストに載っていない場合には、発明を可能とするルータは、明記された目的地にバインディング・アップデート・メッセージを送ることも可能である。

【0061】

【発明の効果】

本発明によって、パケット交換データ・ネットワークのインターネットワーキングにおけるホストが、モバイル・ホストへのグローバル接続性を提供する既存の解決策を使用することを可能とし、これらの解決策を拡張して、接続点を変更するネットワークへのグローバル接続性を提供する。本ドキュメントで開示されている方法を使用することによって、移動するネットワーク間のパケットを、意図された目的地に最小の遅延で配送することができ、さらに、本発明によって提

供される確認方法の使用によって、ネットワーク・エレメントは、それらがさらされるセキュリティの脅威を減少させることができる。

【図面の簡単な説明】

【図 1】

バインディング・エントリの更新 — この図は、ネットワーク・エレメントがバインディング・アップデート・メッセージを受け取った場合に、バインディング・アップデートを更新するために、ネットワーク・エレメントによって使用されるアルゴリズムを示すものである。

【図 2】

ルーティング・ヘッダの構築 — この図は、モバイル・ノードに直接パケットを配送するためのルーティング・ヘッダを構築する場合に、ネットワーク・ホストによって使用されるアルゴリズムを示すものである。バインディング・エントリは、再帰的にモバイル・ノード及びそのアクセス・ルータの気付アドレスを取得するために使用され、スタックは、これらのアドレスを格納するために使用されて、ルーティング・ヘッダを構築する場合、逆の順番でアドレスを戻すことが可能である。

【図 3】

ルータによるセキュリティ確認 — この図は、ルータに接続されたローカル・ネットワークのうちの 1 つに転送されるパケットをルータが傍受した場合に、ルータによって行われるステップを示すものである。このテストのシーケンスによって、セキュリティ脅威に対するローカル・ネットワークの脆弱性を減らすことが可能となる。

【図 4】

モバイル・ノードによるセキュリティ確認 — この図は、モバイル・ノードがパケットを受け取るときにモバイル・ノードによって行なわれるチェックを図示するものである。ここに記述された確認のプロセスは、セキュリティ脅威にモバイル・ノードの脆弱性を減らすことが可能とする。

【図 5】

直接転送要求の取り扱い — この図は、外部に向かうパケット、すなわち、

ルータに接続されたローカル・ネットワーク内のノードによってグローバルなデータ通信網上の他のホストに出されるパケットを処理するために、ルータによって使用されるアルゴリズムを説明するものである。

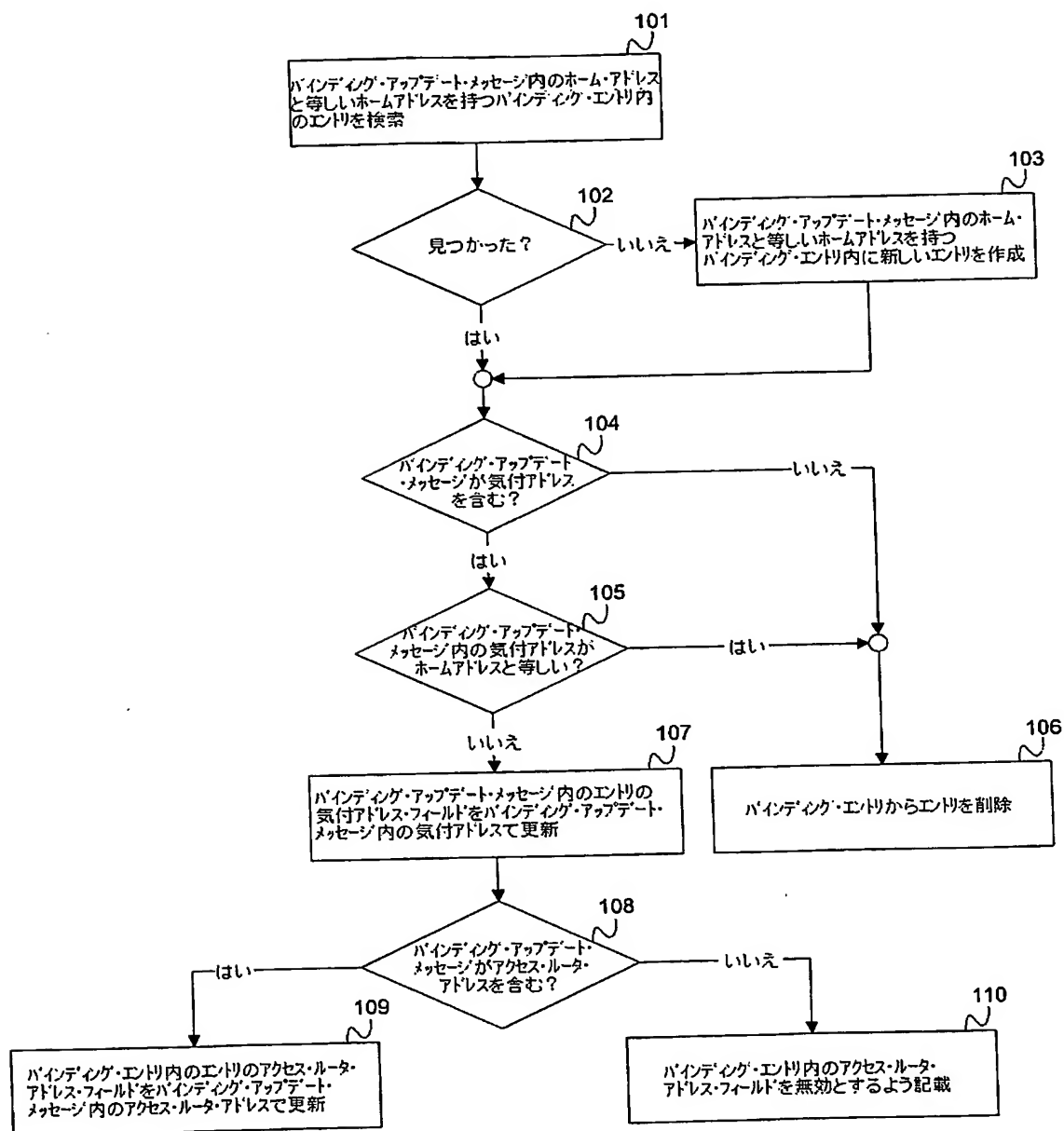
【図 6】

他のホストによるセキュリティ確認 — この図は、明記されたソース・アドレスを持つパケットが前回のバインディング・アップデートによって、パケット・ヘッダに含まれるホーム・アドレスにリンクされることをチェックするために、ホーム・エージェント又は対応ノードなどのネットワーク・ホストによって使用される確認のプロセスを示すものである。図で基本的に示されるアルゴリズムは、ソース・アドレスとホーム・アドレスとの間の関係を確認するため、繰り返しバインディング・エントリを調査するものである。

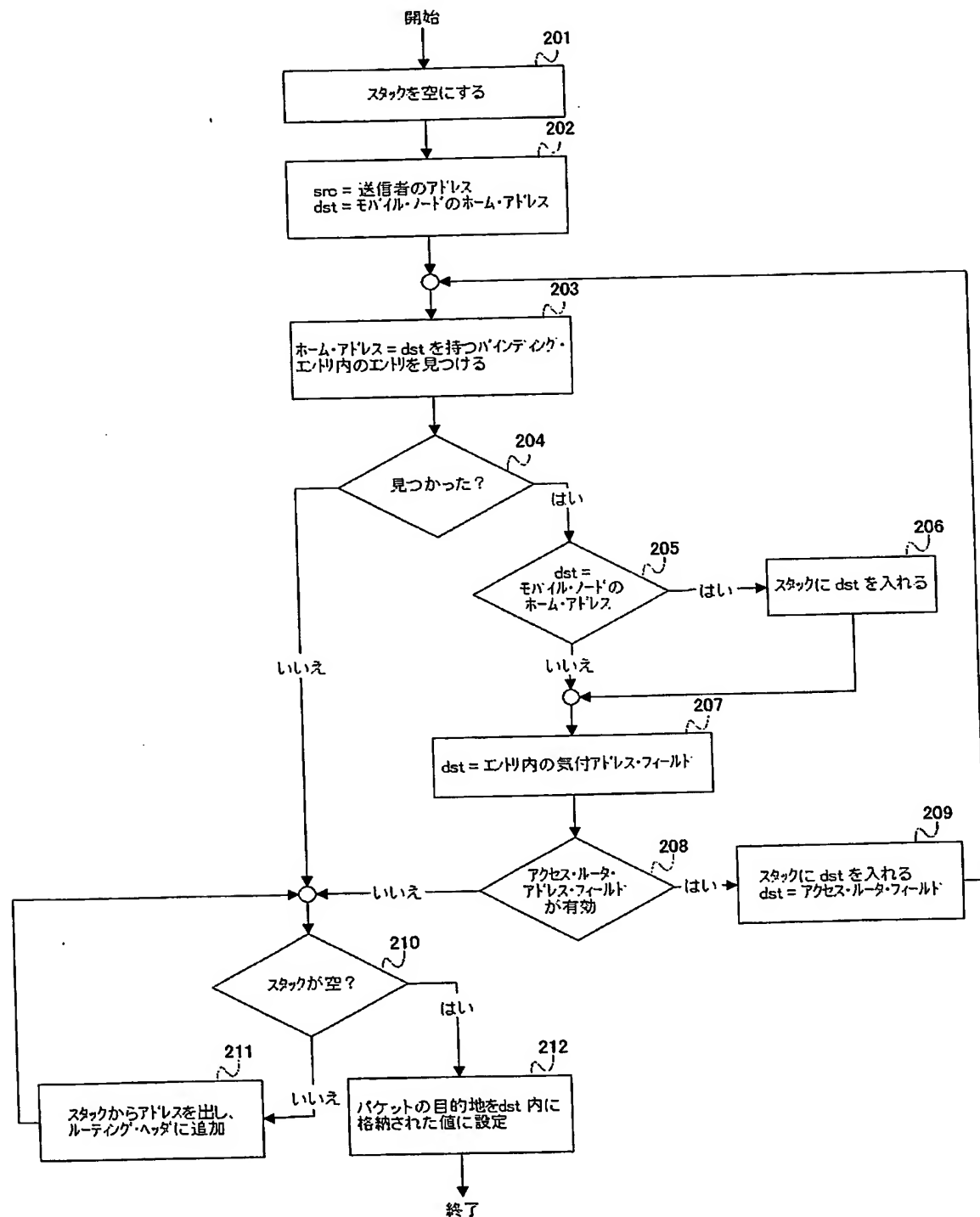
【書類名】

図面

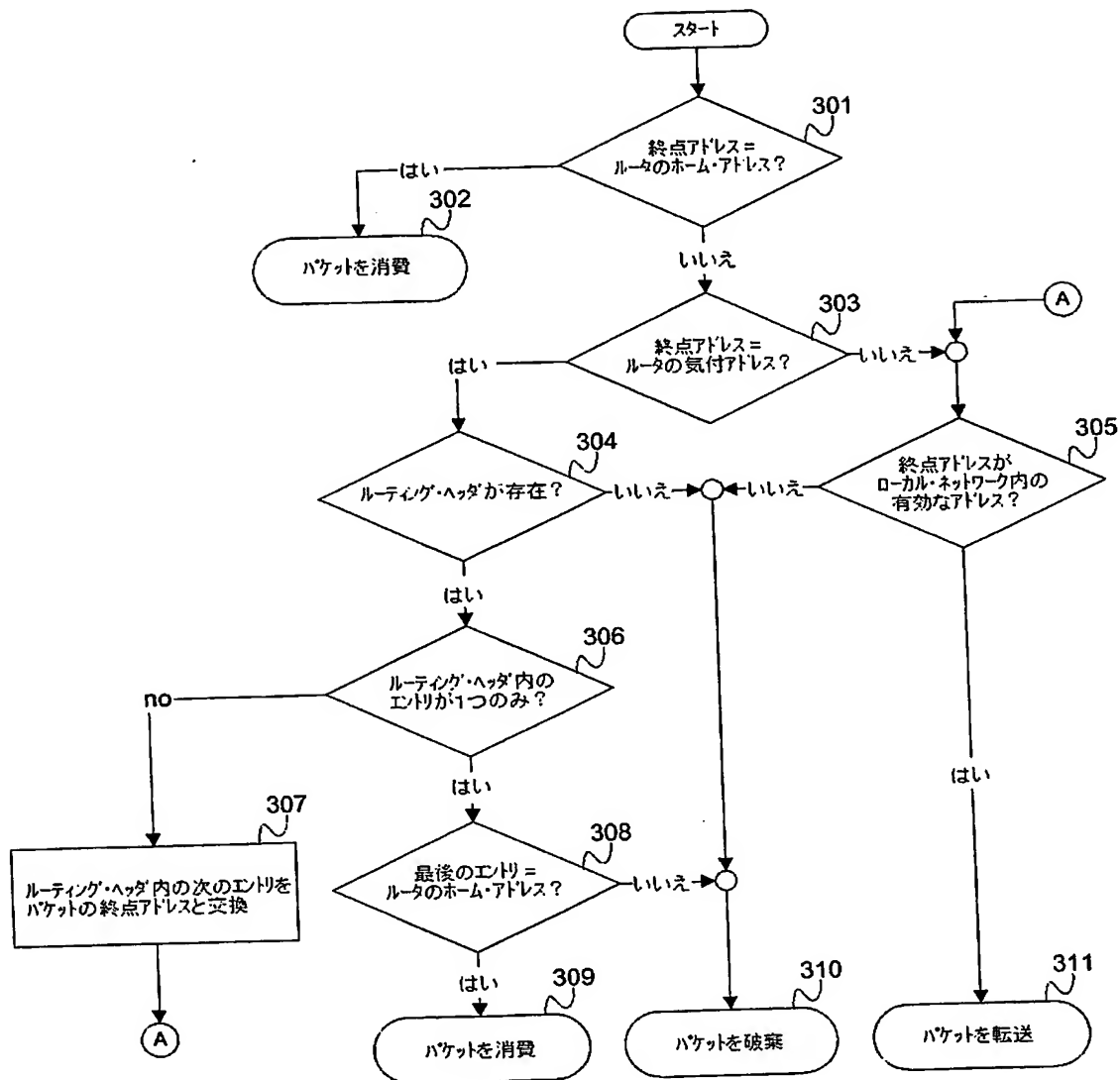
【図 1】



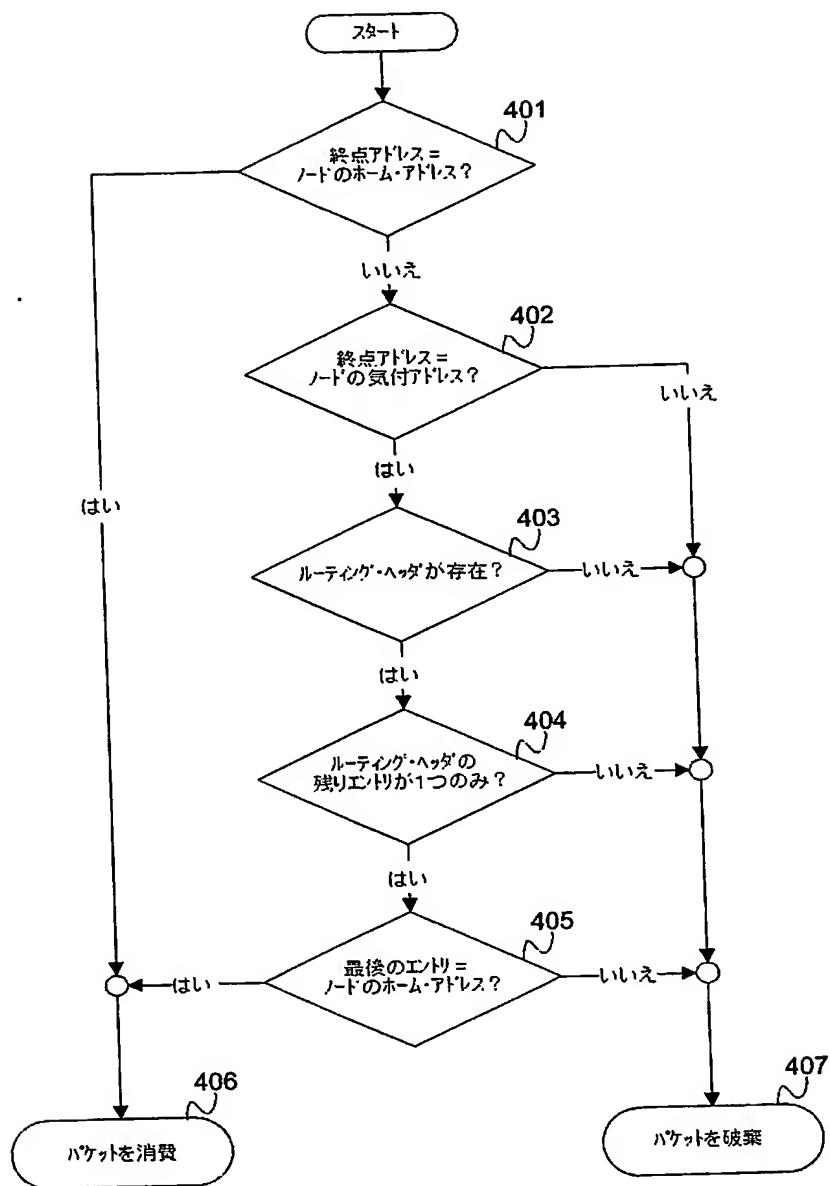
【図 2】



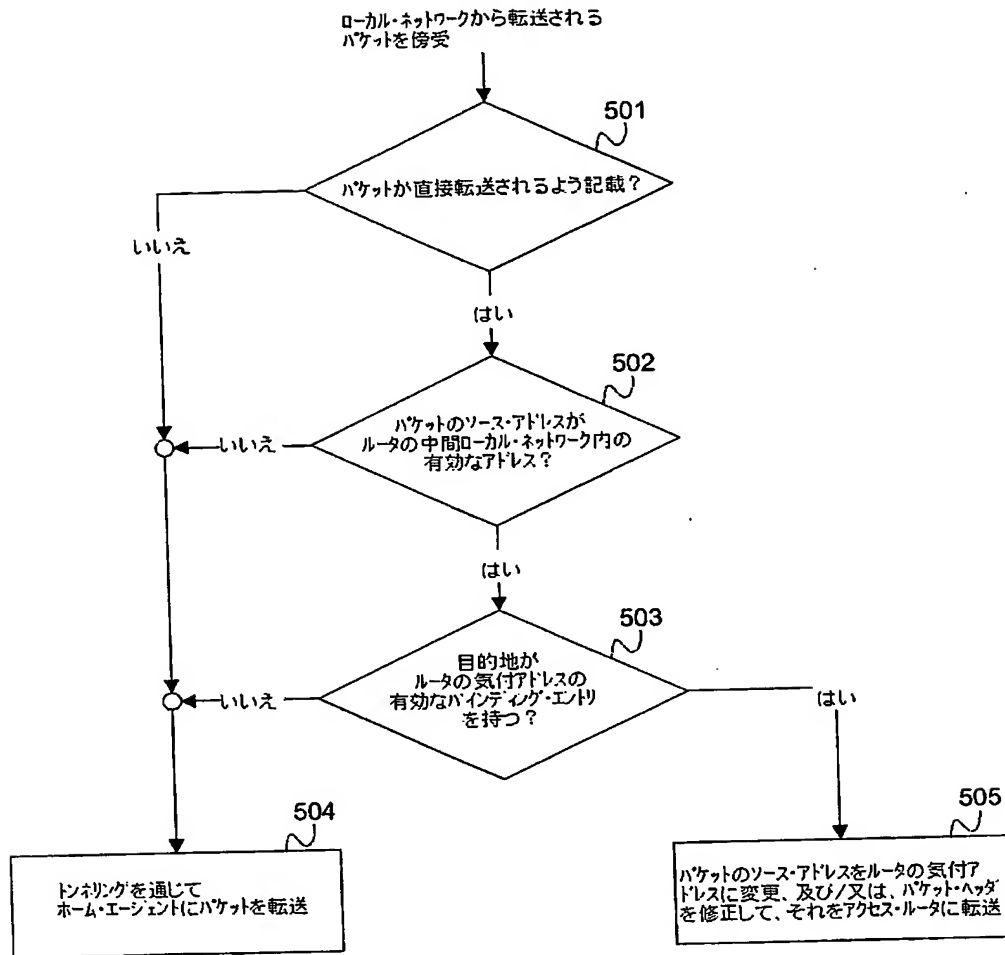
【図 3】



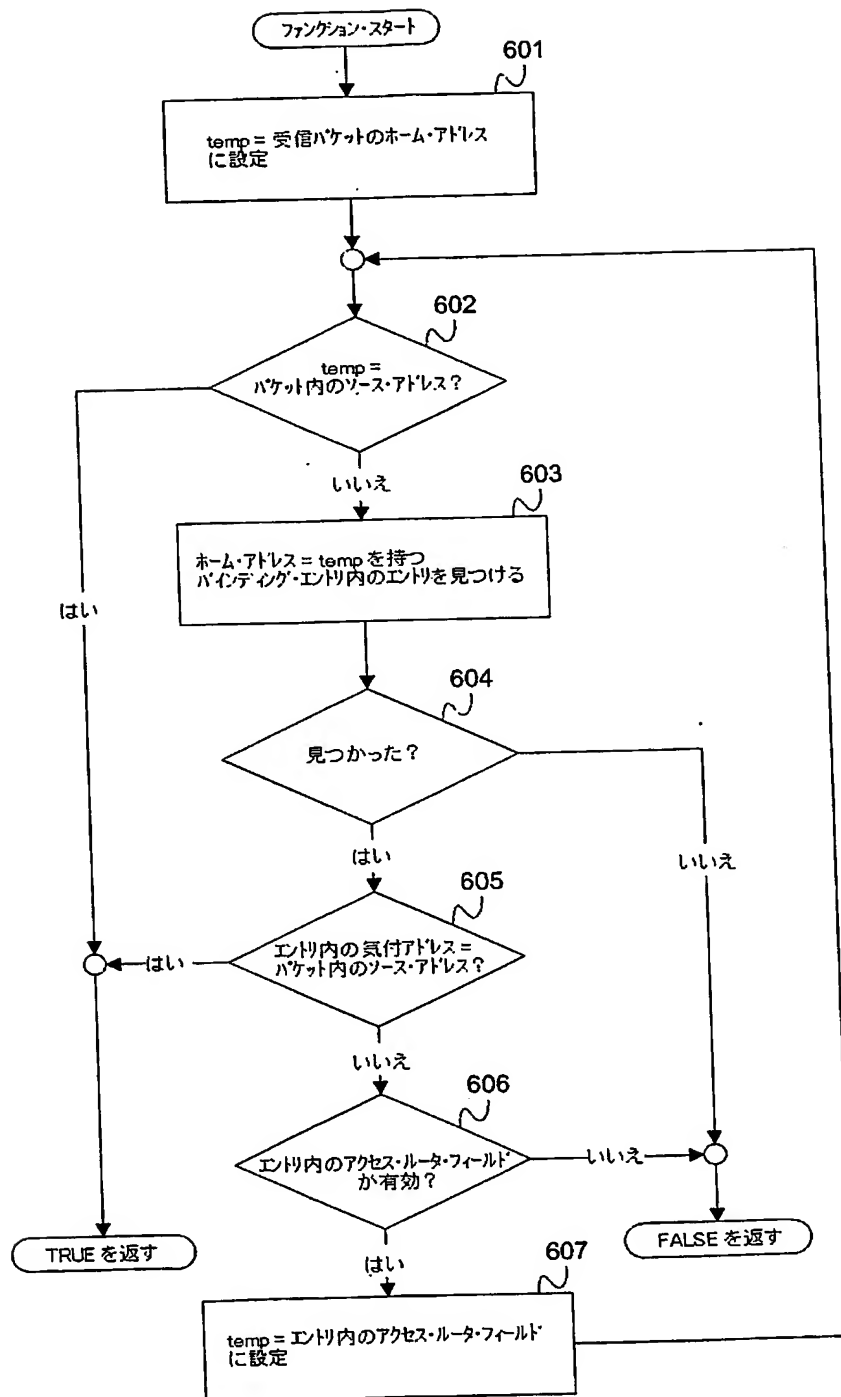
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 接続点を変更するネットワークへのグローバル接続性を提供することに関する発明が開示されており、本発明は、パケット交換データ通信網のインターネットワーキングでの異なる種類のノード内で使用されるメカニズム及び方法を提供する。

【解決手段】 ノードの種類は、グローバルなデータ通信網への接続点を変更するモバイル・ホスト、移動するネットワークの外部ネットワーク側インターフェイスを制御するモバイル・ルータ、及び、モバイル・ホスト及びモバイル・ルータと通信し、グローバルなデータ通信網上の他のホストである。これらのアルゴリズム及びメカニズムを工夫して、移動するネットワーク間のパケットを最小の遅延で、意図された受信者に配送することが可能となり、さらに様々なメカニズムも導入し、開示された方法を使用しているノードが、セキュリティを脅かされにくくなる。

【選択図】 図1

認定・付加情報

特許出願の番号

特願 2002-303879

受付番号

50201920283

書類名

翻訳文提出書

担当官

第七担当上席

0096

作成日

平成14年12月24日

<認定情報・付加情報>

【提出日】

平成14年12月18日

次頁無

特願2002-303879

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

[変更理由]

住所

氏名

1990年 8月28日

新規登録

大阪府門真市大字門真1006番地

松下電器産業株式会社